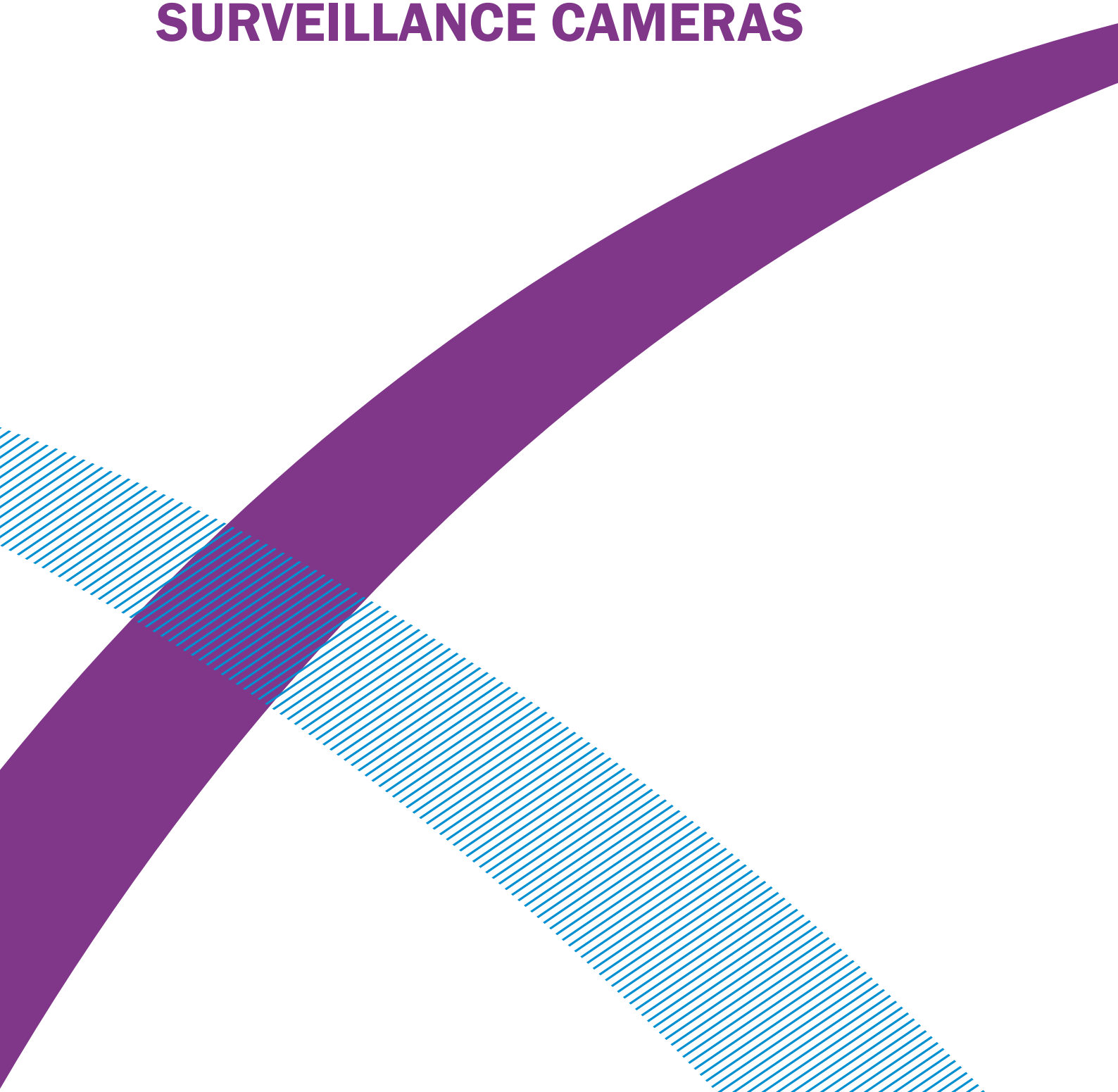
Home Office

CONSULTATION ON A CODE OF PRACTICE RELATING TO SURVEILLANCE CAMERAS



CONTENTS

1. MINISTERIAL FOREWORD 3
2. ABOUT THIS CONSULTATION 4
3. BACKGROUND 6
4. GOVERNMENT APPROACH TO REGULATORY FRAMEWORK 12
5. CODE OF PRACTICE 13
6. FUTURE DEVELOPMENTS 17
7. CONSULTATION CRITERIA 18

ANNEX A - EXISTING PRIMARY LEGISLATION 19

Topic of this consultation:	Following the Government's commitment to further regulate Closed Circuit Television (CCTV) the Protection of Freedoms Bill provides for the development of a Code of Practice relating to CCTV, Automatic Number Plate Recognition (ANPR) and other surveillance camera systems, and the appointment of a Surveillance Camera Commissioner to monitor its operation.
Scope of this consultation:	This paper sets out the Government's intended approach to the development of a Code of Practice – in particular issues for inclusion, and how adoption of the Code by system users can be promoted. The paper invites suggestions as to other topics that might be included in the Code or are relevant to its future operation, and also seeks views on how regulation might be further developed in future.
Geographical scope:	These proposals extend to England and Wales. Where they impact on devolved responsibilities we will work closely with the Welsh Assembly Government on any resulting policy development.
Impact assessment (IA):	An initial Impact Assessment has been prepared and will be published separately.
To:	Members of the public; public and private sector owners and operators of CCTV, ANPR and other surveillance camera systems; industry; interest groups.
Duration:	The consultation starts on 1 March 2011 and ends on 25 May 2011.
Enquiries:	Home Office CCTV Consultation PPPU 5th Floor Fry Building 2 Marsham Street London SW1P 4DF

How to respond:	You can respond online at: CCTVandANPRconsultation@homeoffice.gsi.gov.uk or if you prefer send written comments to the above address.
Additional ways to become involved:	This will be an online consultation exercise. A PDF consultation document will also be available to download online. Please contact the Home Office at the address above if you require information in any other format such as Braille, large font or audio
After the consultation:	The consultation responses will be used to help inform the development of the proposed Code of Practice (subject to passage of the relevant provisions of the Protection of Freedoms Bill).
Getting to this stage:	An interim CCTV Regulator was appointed in December 2009 to advise on CCTV issues and to consider, amongst other things, the need for and potential elements of, a regulatory framework for CCTV. The proposals in this paper relating to the development and implementation of a Code of Practice build on the results of his work to date.
Previous engagement:	The Interim CCTV Regulator has previously consulted with key public sector bodies with an interest in CCTV through the National CCTV Strategy Board. He has also had some informal consultations with industry and has examined existing schemes and examples of good practice already in operation at local level.

1. MINISTERIAL FOREWORD

Recent years have seen a dynamic growth in both the volume and capability of technology of all types. This has had a significant impact on all parts of society in terms of the way in which we are able to interact and conduct our affairs. Such developments are frequently beneficial, for example in keeping the public safe, enabling us to conduct business more quickly and economically, and allowing easy access to diverse services and entertainments. There are however, also potential disadvantages to such developments, including the extent to which private lives are exposed to ever greater scrutiny by other individuals, organisations or the State, leading in some instances to a potential exposure to criminality, or more generally, to an erosion of personal privacy.

The Government is committed to ensuring that the tools and technology which contribute to public security, the prevention and detection of crime, and which serve to reassure the public, remain fully available for these purposes. The use of such tools has, however, increased dramatically in recent years and independently of a bespoke regulatory framework. This has given rise to legitimate concerns about the extent and purpose of State intrusion into people's lawful business, and the retention, security, and use of the data collected.

We are determined to ensure that the significant increases in State surveillance which have occurred over the last decade should not go unchecked. Our Coalition Agreement sets out a package of measures which will roll back the over-intrusive powers of the State. We are committed to restoring and preserving our historic and valued traditions of freedom and fairness.

As part of that package we have introduced provisions in the Protection of Freedoms Bill providing for a new regulatory framework for surveillance cameras. This gives effect to our Coalition Agreement commitment to further regulate Closed Circuit Television (CCTV). The approach we are adopting also encompasses other types of camera surveillance – in particular Automatic Number Plate Recognition (ANPR) technology given its many similarities to CCTV – but also providing scope to deal with other emerging technologies as necessary.

A cornerstone of a free and confident society is the State's duty to ensure that its citizens are sufficiently protected so that they are able to conduct their legitimate business in safety and security. We do not intend therefore, that anything in our proposals should hamper the ability of the law enforcement agencies or any other organisation, to use such technology as necessary to prevent or detect crime, or otherwise help to ensure the safety and security of individuals. What is important is that such use is reasonable, justifiable and transparent so that citizens in turn, feel properly informed about, and able to support, the security measures that are in place.

Our approach to establishing a new regulatory framework is therefore intended to provide a means through which public confidence in CCTV, ANPR, and other such systems, is improved by ensuring that there is proper transparency and proportionality in their use. We also aim to ensure that the considerable investment in technologies such as CCTV yields worthwhile returns by ensuring that they are operated as efficiently and effectively as possible. At the same time we are committed to minimising new regulatory burdens, so our proposals aim to introduce safeguards in a measured and proportionate way, which takes account of the current national state of development in this area.

This consultation provides further details of our proposals and seeks suggestions in particular, on the development of an effective Code of Practice on surveillance cameras.

2. ABOUT THIS CONSULTATION

This paper sets out some of the key issues associated with the increased prevalence of CCTV and ANPR use, and describes how the provisions set out in the Protection of Freedoms Bill are designed to address these. The initial focus is the development of a new, comprehensive, Code of Practice designed to promote clarity and consistency in the future use of such technology.

This consultation document is concerned with the overt use of systems such as CCTV and ANPR in public or semi-public places where people can generally either see a camera, or are informed about its presence. It does not cover covert surveillance techniques, which are legislated for through the Regulation of Investigatory Powers Act (RIPA) 2000.

We expect this consultation to be of relevance to a wide range of system developers, users, and members of the public. It therefore seeks the views of CCTV and ANPR operators in the public and private sector, relevant industry members, interest groups and members of the public, on the potential content and effective implementation of a new Code of Practice in relation to surveillance camera systems. It is intended in the first instance that the Code of Practice will focus on addressing issues relating to the use of surveillance cameras by the State and other organisations in areas to which the public have general access. (In other words, the use of such technology in an essentially private, individual capacity will not initially be a priority). In keeping with the Government's intended incremental approach to this issue, however, it also seeks views on issues not immediately or directly addressed by such a Code, but where further regulation might in future be necessary or beneficial.

DEVOLVED ADMINISTRATIONS

Provisions included in the Protection of Freedoms Bill introduced in Parliament in January 2011 apply only to England and Wales. Discussions are underway with the Welsh Assembly Government on development of the Code with respect to any issues involving devolved responsibilities.

2.1 RESPONSES: CONFIDENTIALITY & DISCLAIMER

The information you send us may be passed to colleagues within the Home Office, the Government or related agencies.

Information provided in response to this consultation, including personal information, may be subject to publication or disclosure in accordance with the access to information regimes (these are primarily the Freedom of Information Act 2000 (FOIA), the Data Protection Act 1998 (DPA) and the Environmental Information Regulations 2004).

If you want other information that you provide to be treated as confidential, please be aware that, under the FOIA, there is a statutory Code of Practice with which public authorities must comply and which deals, amongst other things, with obligations of confidence.

In view of this it would be helpful if you could explain to us why you regard any information you have provided as confidential. If we receive a request for disclosure of the information we will take full account of your explanation, but we cannot give an assurance that confidentiality can be maintained in all circumstances. An automatic confidentiality disclaimer generated by your IT system will not, of itself, be regarded as binding on the Department.

The Department will process your personal data in accordance with the DPA and in the majority of circumstances this will mean that

your personal data will not be disclosed to third parties.

Should you require a copy of this consultation paper in any other format, e.g. Braille, Large Font, or Audio please contact the consultation team (details on page 1).

3. BACKGROUND

3.1 CURRENT REGULATION

This arena is not entirely unregulated. Details of the principal legislative provisions with relevance to CCTV and ANPR are set out in Annex A. Such provisions tend, however, to address specific (and therefore limited) aspects of the use of such systems. In the meantime, greater affordability and technological advances have generated a significant growth in the use of such technology independent of any comprehensive strategic approach, leading to a wide variety of applications and standards. Some of the complexities, benefits and challenges stemming from such historical developments are described below.

3.2 CLOSED CIRCUIT TELEVISION (CCTV)

CCTV has become a familiar feature of modern life and is commonplace in both public spaces and those privately owned areas to which the public has ready access. It can be seen in operation daily in our high streets, on public transport, at stations and airports, and in banks and shops. Images from CCTV are frequently seen in our own homes, via television, in appeals for information on serious crimes, or when reporting on major incidents.

The CCTV landscape is complex in that, while CCTV images are perhaps most commonly associated with the police, the majority of publicly owned, public place CCTV systems are local authority systems. In addition, many other systems are owned and operated by the private sector in locations where the distinction between public and private space is blurred, including for example privately owned premises which the public is actively encouraged to visit (shopping centres, business premises, public transport and sporting venues). In many local areas, there has been a deliberate integration and networking of publicly and privately owned systems in recognition of the blended nature of the space in which we conduct many of our day to day activities and in order to maximise the benefits of CCTV coverage of these areas.

CCTV may also be used in wholly private spaces to which the general public does not normally have access, for example factories (for the purposes of monitoring production or hazardous processes), or private dwellings (for personal security). In such instances there may sometimes be limited extension of such technology into public areas such as footpaths or roads bordering the property, or neighbouring private property.

While many CCTV cameras are fixed in a single location, CCTV can also be mobile (mounted in vehicles), worn on the body or "redeployable" (erected for a temporary period and then removed) – adding to its versatility and the situations in which it can be used.

BENEFITS

In the public and semi-public arena CCTV has many potentially useful purposes.

I. CRIME PREVENTION AND DETECTION

Many of the stated objectives for local council owned CCTV relate to crime prevention and crime detection. In some circumstances, the presence of CCTV may in itself act as a deterrent (either alone or in combination with other factors), reducing the incidence of crime. Some, however, argue that it may simply displace crime to other areas (and there is mixed evidence as to whether this is the case[1]).

CCTV can be very useful for identifying potential or emerging trouble - for example antisocial or violent behaviour as the pubs or clubs close, or following sporting events - enabling the police to be directed quickly to where they are needed. CCTV can also track mobile incidents across an area (for example stolen vehicles, or fleeing suspects) again

1 "Effects of Closed Circuit Television Surveillance on Crime" Brandon C Welsh, David P Farrington (Campbell Systematic Reviews 2008:17)

enabling resources to be deployed more effectively in response.

Images captured by CCTV can be of significant evidential and forensic value in identifying perpetrators (dependent on the quality of images), or in some cases clearing initial suspects of any involvement. They can also be valuable for informing lines of inquiry and investigation, for example, by establishing the movements of a victim or suspect or spotting suspicious behaviour.

II. COUNTER- TERRORISM

CCTV has had a very important role in counter terrorism measures, in particular:

- monitoring, surveillance and intelligence gathering;
- assessment and response to a possible incident;
- assessment and response following an actual incident; and
- forensic and evidentiary analysis after an incident.

Some of the intelligence gathering may be undertaken through covert surveillance (see Regulation of Investigatory Powers Act (RIPA) 2000 – Annex A), but overt public space CCTV has also proved valuable in investigations - including for example into the terrorist attacks in London of 7 and 21 July 2005.

III. CRIMINAL JUSTICE

CCTV footage or images may form part of the evidence shown to juries to assist them in reaching their verdicts, or to members of the judiciary in order to assist with sentencing decisions.

IV. TRAFFIC MANAGEMENT

Cameras are used in a variety of ways on our roads. Some cameras are designed to monitor traffic flows and identify traffic problems caused by congestion or failed signals etc. Often, such cameras do not record any images and are simply used for monitoring general traffic volume and flow. Other cameras are used for traffic enforcement such as monitoring bus lanes, box junctions, one way streets and parking restrictions, and may capture and record images.

IV. HAZARD MANAGEMENT AND PERSONAL SAFETY

CCTV is used extensively on and around public transport where in addition to general security it can also help to identify potential hazards or accidents (e.g. obstacles, failed signalling equipment, individuals jumping or falling onto railway tracks or underneath vehicles). It can be used to help track vulnerable members of the community (such as missing patients with mental health problems) and to alert the emergency services to someone requiring assistance. It may further assist the emergency services, such as the fire brigade, when responding to major incidents - by identifying particularly hazardous areas or evacuation routes. Cameras may also be used in certain areas to monitor potential environmental hazards such as flood risks.

V. PEOPLE AND PROPERTY

CCTV is also (and increasingly) used in a very wide range of individual institutions and businesses (some public and some private) to which the public, or a section of the public, have legitimate access. These include schools, hospitals, public transport, sporting venues, museums, banks, shops, petrol stations, parks, airports, and businesses. CCTV in such circumstances is used for a wide variety of security and safety reasons - to safeguard property from vandalism or burglary, to deter or detect theft of goods or valuable items, for crowd control and safety, for research purposes; to monitor wildlife or pests; to protect staff/patients/pupils from

violence or other criminal acts, to detect shoplifting, petrol theft etc.

CHALLENGES

CCTV does not always provide the benefits expected of it. Despite the proliferation in CCTV, its value to the police when investigating crime or major incidents is often limited due to poor camera positioning, poorly maintained equipment or lack of recording facilities. Where images are captured, a particular problem is the variety of and quality of formats in use to record and store these, meaning that it can be extremely time consuming and costly for the police to retrieve and convert images into a format that can easily be viewed or used in court proceedings. There also the challenge around identifying and recovering all relevant images associated with an investigation within tight timescales, and before it may be routinely deleted from systems.

State of the art CCTV systems or networks can be expensive to set up and have ongoing running, maintenance and up-grading costs. There is conflicting data and information about the usefulness of CCTV for crime prevention and reduction which makes it important to consider carefully the value of any new systems and to evaluate existing systems.

Another challenge is that modern digital technology is on the cusp of revolutionising the use of CCTV: affordable high resolution systems with powerful zoom potential, small discrete cameras, 360 degree vision, wireless and internet networks facilitating mobility and cheap installation, and effective video analytics software (for example, facial recognition) are coming closer to being an established part of the CCTV landscape. New uses for systems, for example in taxis, are a natural part of industry growth.

The use of CCTV or similar systems by private individuals can often be a valuable and important tool in ensuring personal safety (for example where individuals are subject to ongoing harassment or antisocial behaviour). However, for some law abiding individuals the use by neighbouring properties of surveillance equipment can be considered intrusive, especially if it overlooks areas of their own property (such as shared boundaries).

Given the wide variety of uses to which CCTV can be put, and the variable degree of potential intrusion into daily lives which needs addressing, devising a single and sufficiently flexible legislative framework is challenging. For example, major transport system operators (e.g. Transport for London (TfL)) own large numbers of cameras; however, where the images are unrecorded there is a low risk of breach of data protection legislation or disproportionate impact on human rights. In contrast, where personal images are captured and stored there is a potentially higher risk around issues such as privacy and data security, potentially in breach of the Data Protection Act (DPA). This is heightened where images are captured in particularly sensitive areas and where expectations of privacy are generally high, such as schools and hospitals. The DPA already governs many aspects of such use and in 2008 the Information Commissioner published a CCTV Code of Practice highlighting this.

3.3 AUTOMATIC NUMBER PLATE RECOGNITION (ANPR)

Automatic Number Plate Recognition (ANPR) technology shares some characteristics with CCTV in that it uses cameras to capture and store images. However, a distinction can be made in terms of its capability in that it is also able to interrogate other data sources, link relevant information and report on this in real time. It is also significantly easier to search than current CCTV technology.

ANPR cameras can be static or mobile. ANPR works by capturing images of vehicles and converting into text the parts of the images that appear to be number plates. These registration numbers may then be stored and compared to databases of vehicles of interest.

Like CCTV, ANPR has a number of uses and users including:

- the Police Service, for real-time targeted interception and post-incident investigation;
- Her Majesty's Revenue and Customs and the Serious Organised Crime Agency, for investigations;
- Local Authorities (usually linked to their local police force), for enforcement or monitoring purposes;
- the Driver and Vehicle Licensing Authority (DVLA) and Highways Agency for vehicle and road monitoring;
- the Private Sector for security, revenue enforcement and access control on garage forecourts, car parks, etc.

In the case of police use of ANPR, unlike CCTV, the primary source of ANPR data is the Police Service's own camera infrastructure. Each force owns cameras that feed data into a locally-managed back office. Data is retained there and also forwarded on to a National ANPR Data Centre (NADC). The vehicle registration mark (VRM), time and location of sighting, along with an image of the number plate (for checking purposes) and an overview image of the vehicle are stored (although the latter is not forwarded to the NADC). The main databases which are searched for a match are:

- the Police National Computer (PNC) including vehicles that have been stolen or linked to crime;
- local force databases of vehicles of interest to the police;
- MIDAS (Motor Insurance Database for ANPR Systems) regarding uninsured vehicles;
- DVLA databases to check for vehicles without a current VEL or current registered keeper;
- other national databases (e.g. national operations and counter-terrorism).

Where a match occurs, authorised staff receive a notification of the event and there is the opportunity to provide an appropriate response, for example to task patrols to intercept the vehicle.

ANPR cameras are also used by local authorities and the Highways Agency for the purposes of road/congestion charging and traffic management more generally. Increasingly they are also used by businesses such as petrol stations, shopping centres and car parks for security or crime reduction purposes.

BENEFITS

ANPR has been shown to be a powerful tool with a wide range of uses by the police and other law enforcement bodies and by private sector organisations.

Police use of ANPR helps to protect law-abiding citizens on the road from drivers who may be banned or uninsured or driving unroadworthy vehicles. It can be used to identify individuals wanted by the police, for example having breached bail conditions or being unlawfully at large. It can help to disrupt the activities of known criminals by denying them unfettered use of the road system. It can be used for investigative purposes following crimes. For example, the use of ANPR was valuable in tracking down the killers of PC Sharon Beshenivsky. Here, ANPR differs significantly

from CCTV, because ANPR data is more easily searchable. Accordingly, its longer retention can be particularly helpful in police investigations although there should be public transparency in relation to the length of any retention periods and these should be consistent with the fifth data protection principle that data processed for a particular purpose, should not be kept for longer than is necessary for that purpose.

ANPR can also be used in targeted intelligence operations to identify and track individual suspects or groups of suspects believed to be involved in organised crime or terrorism.

In 2006/7[2], ANPR led to:

- the arrest of 20,592 individuals
- the identification of 52,037 vehicle related document offences
- the seizure of 41,268 vehicles for document offences
- the identification and recovery of 2021 stolen vehicles.

Total vehicle seizures have increased since 2006, when police were first granted the necessary powers to seize uninsured vehicles under section 165 of the Road Traffic Act. In 2007 there were 150,000 seizures nationwide; in 2008 this had risen to 185,000[3]. Removing uninsured cars from the road contributes to a reduction in road traffic accidents - more than 20,000 people are injured each year in accidents involving uninsured and untraced drivers. Uninsured driving is also estimated to cost the UK about £500 million each year, adding an extra £30 to every insurance premium to pay for the cost of uninsured drivers. As a result of the police effort to combat uninsured driving since 2005, largely but not only via ANPR, the Motor Insurers' Bureau has recorded a reduction in claims relating to uninsured driving of 22% between 2006 and 2010 nationally.

CHALLENGES

Like CCTV, the use of ANPR has developed in the absence of a specific statutory or regulatory framework leaving scope for ambiguity as to its purpose and usage. With the pace of development of technology, there is the potential for the use of ANPR to outgrow its original strategic aims. For example, it is technically possible, in some cases, to identify the occupants of vehicles through the images captured via ANPR and CCTV technologies, although this is not the main function of the systems. The volume of data captured daily by police ANPR is also significant – between 10 million and 14 million reads per day.

While ANPR has generally proved accurate and helpful in avoiding the stopping, unnecessarily, of law abiding drivers, it is not without weaknesses, relying as it does on the accuracy and timeliness of the databases which it interrogates.

There are strict ACPO guidelines on police use of ANPR. The guidelines enshrine a set of safeguards to ensure the correct use of both the technology and the gathered data. Full audit trails such as records of data access, alteration or deletion are automatically generated and retained to ensure compliance with the national guidelines. Nevertheless given the volume of records captured, the Information Commissioner has expressed concerns about the size of the NADC. ACPO is currently working with the Information Commissioner's Office to refine the current retention criteria and guidance.

There is much less clarity around the use of ANPR by private companies, for example in monitoring private premises and car parks

2 Police Standards Unit. Evaluation of Automatic Number Plate Recognition 2006/2007, Apr 2007. PA Consulting Group.
3 NPIA. ANPR Update. April 2009.

and how data is then used or exchanged with other parties. Whilst the Police Service has agreed standards for the quality of data it collects, no such standards exist for private companies. The lack of overarching regulation of ANPR systems makes it difficult for law enforcement agencies to use ANPR data collected and stored by private organisations where this might be valuable for active investigations.

3.4 OTHER SURVEILLANCE CAMERA SYSTEMS

Ongoing technological developments inevitably lead to refinements to existing technology and the way it may be used as well as to certain niche or more novel technology. At the more familiar end of the scale, this would, for example, include the mounting of cameras in helicopters and aircraft, or "body worn" personal video cameras used by individual officers in particular situations, and at the other end to emerging technology such as remote controlled unmanned airborne vehicles.

While such applications may not currently be in widespread use, there is scope for their unchecked proliferation, and attendant risks if they are not considered within any overarching strategy.

4. GOVERNMENT APPROACH TO REGULATORY FRAMEWORK

In the light of the complexities of the existing landscape and the wish to avoid imposing unreasonable or impracticable bureaucratic or financial burdens on organisations, the Government proposes to take an incremental approach to bringing greater consistency and rigour to the use of such technology. The Government therefore intends to produce a new Code of Practice relating to the development and use of CCTV, ANPR and other surveillance camera technologies, and to appoint a Surveillance Camera Commissioner to promote and monitor its implementation.

The new Code will provide the overarching framework for moving to a consensus on the approach to such technology. Where it already exists, this will draw on relevant existing good practice guidance (such as that developed on CCTV by the Information Commissioner). It will also address the gaps or contradictions in current practice and guidance, with the aim of achieving a comprehensive document encompassing practical advice and good practice, relevant to both users and subjects of surveillance cameras. We intend that the Code will be drawn up in full consultation with interested parties, of which this initial consultation forms the first stage. This is intrinsic to producing a Code which will prove of genuine value to interested parties and thereby secure buy-in and voluntary adoption.

The role of the Surveillance Camera Commissioner will be to promote adoption of the code, monitor its impact and provide advice about it to interested parties. He will act as an independent assessor of the effectiveness of the code in achieving its objectives, reporting annually on this to Ministers.

While initially only local authorities and police forces will have a statutory duty to have regard to the Code in their use of surveillance camera systems, we hope that the Code will be widely adopted as the standard for such operations. If so, this will form the foundation for achieving greater overall consistency in the approach to the use of CCTV and similar applications.

Development of a Code will provide the opportunity to ensure that basic principles are clearly established while more complex issues are properly considered and worked through to an agreed position. Widespread adoption of a common Code will have the effect of gradually raising standards to a common level. Articulating principles via a Code which can be amended as necessary also allows greater flexibility to adapt to and incorporate developing applications and new technology.

The effectiveness of the Code will be kept under review by the new Surveillance Camera Commissioner. If it is considered that insufficient progress is being made in respect of Government aims in this area, we will consider further regulation, including extending the numbers of types of organisations required to have regard to the Code, or making aspects of the Code itself mandatory.

Finally, although many of the principles of the Code should be relevant to anyone considering the use of surveillance cameras, initially the focus will be on addressing concerns around the use of such technology in areas to which the public have ready access rather than being specifically directed at individual members of the public who may use CCTV for example to protect their homes. However, as part of its incremental approach to addressing the question of general surveillance the Government believes that this is one area that should be kept under review and welcomes views on this as part of this consultation (see section 6).

5. CODE OF PRACTICE

5.1 GENERAL

The Protection of Freedoms Bill contains an initial, but non exhaustive, list of the types of issues the Code may seek to address. This document provides further detail on some of the matters that the Code might include. As previously mentioned, it is intended that the detail of the Code will be developed in consultation with interested parties. The following proposals are not therefore, intended to be definitive or exhaustive and views on what aspects of any particular of issues should be covered, how they might most helpfully be presented and identification of additional issues that should be considered for inclusion are welcomed. Broadly, we intend the Code to be an A-Z reference document of pertinent facts and information to help all interested parties to get the best out of their involvement with surveillance cameras, whether as providers, users, operators or subjects.

The precise format of the Code will need to be considered further as it develops. There will be a balance to be struck between comprehensiveness, and convenience and ease of use. It may be possible in part to frame significant parts of the Code in terms of general principles applicable to any form of surveillance camera use. However, specific provisions may need to be included for different types of surveillance camera (for example in respect of CCTV or ANPR) given their slightly different uses and capabilities.

5.2 CONTENTS

PRE-PLANNING

Central to the Government's aims for the ongoing and future use of surveillance cameras is proportionality of use. This suggests that anyone considering the use of such technology should first undertake a thorough assessment of the purpose, likely value, and wider impact of such a course of action and determine in the light of that whether or not to proceed. There are a wide range of means by which this could be achieved and the Code might, for example, include checklists and examples of good practice to assist organisations in asking themselves the right questions and coming to a balanced conclusion. These might for example include:

- whether the proposed installation is part of a developed and integrated strategy;
- clarity on the main purpose and perceived advantages of the use of the technology;
- assessment of whether available technology will meet that purpose in full;
- whether there are alternative means of achieving the same outcomes;
- whether accompanying safeguards (including operating procedures) are already in place or need to be developed;
- impact assessments (including environmental, privacy, disproportionality etc);
- the appropriateness of permanent or temporary/mobile cameras;
- cost benefit analysis or value for money;
- consultation with relevant partners;
- appropriate consultation with the public, or any specific group, most directly affected by any planned surveillance;
- reviews of the continuing need for, or value of, any system installed.

Q. What other preparatory checks or balances should be included?

Q. Do you have examples of existing guidance or good practice in this area that could be drawn on in developing the Code?

STANDARDS

A wide range of equipment and systems are available on the market (particularly in respect of CCTV). The cameras themselves have different specifications and functions, and similarly, where images are recorded, these are stored in different formats. This poses several challenges. Given the resources invested in CCTV and ANPR, it is important that it works reliably and effectively, and crucially, that it captures images which are capable of properly fulfilling the purposes for which the individual systems were intended. This encompasses issues such as image quality (i.e. resolution) and the compression and storage of resulting data.

While some international, European, British and industry quality standards are in existence (and to which manufacturers may already choose to work), there is no single agreed or widely used set of technical baseline standards for CCTV. On ANPR, ACPO has developed its own set of National Standards, but these do not necessarily apply to other operators. Establishing a menu of applicable standards for use both by industry and users could have a range of benefits.

The Government has no intention of requiring that all users must upgrade their systems, but the adoption of industry standards would not only provide assurance for customers that their systems would operate as claimed; it would, over time, promote greater consistency between systems (as they are replaced or upgraded). This would facilitate the integration of systems where this was deemed desirable, reducing the need for technical transfers of data to other formats and making the collection of evidence for law enforcement purposes easier and more efficient. It is also likely that images would be of an improved quality, providing better evidence in criminal proceedings. Industry would also be likely to benefit by being clear about customer requirements, ensuring a level playing field for competition.

The Government would therefore wish to engage with manufacturers businesses and users on the merits and feasibility of developing a range of technical standards for equipment, at national or international level. This should be easily recognisable for users, for example, by the adoption of a British Standard, “kite mark”, or similar established reference.

Q. Do you think it would be beneficial to establish a common technical standards baseline for the surveillance camera industry?

Q. Are there any particular technical issues on which the development of a standard would be especially valuable?

Q. If common technical standards were not developed, how could consistency and performance be improved in other ways?

Q. What drawbacks are there to having common technical standards?

As well as the technical aspects the concept of standards could also be extended to the operation of CCTV systems (e.g. the standards expected of staff, training etc.). Again, some relevant British and international standards already exist which require self, or independent, auditing of systems against key criteria. The Code might promote these as examples of good practice.

Where not already captured in such standards the Code could also seek to deal with expectations on individuals operating surveillance systems or handling the data captured by them, including core training issues.

Q. What other (non-technical) issues might benefit from the adoption or development of key standards?

DATA PROTECTION

There is already very comprehensive and well established legislation and guidance relating to the proper handling of personal data (which includes images gathered from surveillance cameras) under the Data Protection Act (DPA 1998). This is regulated by the Information Commissioner's Office, who has already produced a comprehensive Code explaining its relevance to the use of CCTV.

There is no intention for the new Code, or the role of the new Surveillance Camera Commissioner, to cut across the existing role of the Information Commissioner. There will, however, be a strong overlap of areas of interest and it is intended, and essential, that the respective Commissioners will work closely together to ensure that any issues that arise are properly addressed. Full consideration will need to be given to how best to reflect in the new Code the relevant data protection provisions, and the respective extent of the roles and responsibilities of the two Commissioners in relation to monitoring the operation of the Code and data protection issues. Views on what would be of most assistance to the CCTV user or members of the public in terms of the format for presenting this information would be welcomed.

While the Code is not expected to deal extensively with covert surveillance (which is subject to the requirements of the Regulation of Investigatory Powers Act (RIPA)) it will similarly provide the opportunity to clarify any areas of overlap with the role of the Office of Surveillance Commissioners.

One area in which it may be particularly helpful for the new Code to provide further or refined guidance is in relation to recommended data retention periods, especially, for example, in respect of ANPR data. Guidance on data sharing provisions and restrictions in the context of surveillance camera systems is likely also to be of value.

The Code might also contain or point the way towards appropriate training levels for system operators in the collection, storage and subsequent use of data.

Q. Would it be helpful to combine the existing Information Commissioner's CCTV Code into a new single CCTV code, or maintain a distinction between data protection issues and other technical CCTV operational issues through separate codes?

Q. Are there other issues relating to the collection, storage and subsequent use of data which should be included in the Code?

IV. PROVISION OF INFORMATION

Good practice – as already described in the Information Commissioner's Code for CCTV – suggests that an important way of commanding public confidence is by ensuring transparency of process in the ownership, purpose and use of surveillance cameras (except of course where they are being used under authorisation as part of a covert investigation), although not transparency in relation to the data collected. Some local authorities, for example, publish the locations of public space cameras in their areas.

The Code would present an opportunity to draw together ideas for increasing such transparency including through public consultations, publication schemes, and labelling. The aim should be to enable any individual wishing to know more about an overt surveillance camera to be able to obtain that information easily and readily, whilst the personal data itself is appropriately safeguarded.

The development and publication of effective complaints procedures for existing schemes would also be an important way of addressing public concerns about proportionality of use and data security.

Q. What information do you want to be able to obtain in relation to surveillance camera systems?

Q. What methods are most effective for providing information? Do you have any examples of good practice in this area?

Q. Are there any other issues you think should be included in a Code of Practice?

5.3 IMPLEMENTATION

To address concerns about state intrusion into private lives, we have provided that, in the first instance, the police and local authorities should be required to have regard to the provisions of the Code in their operation of surveillance camera systems. For other bodies, initially at least, adoption of the Code will be a matter of self regulation. We hope however, that since the Code will be developed in consultation with interested parties and will represent good practice and practical advice, organisations will see the benefits of adopting it.

The role of the Commissioner is not one of enforcement; rather, it is to promote the benefits of the Code, help to identify changes that might need to be made to it and report on its effectiveness. If the Code proves ineffective as a way of driving up standards and addressing concerns in this arena, the Government will give consideration to extending the list of organisations required to have regard to the Code current provisions or to introducing further legislative provisions.

Views would be welcomed on how voluntary compliance with the Code can be maximised and whether, in the longer term, there are issues on which it is thought mandatory requirements might be desirable or necessary.

The development of standards might be helpful in this respect and manufacturers might be encouraged for example to remind customers of the existence of the Code when supplying new equipment.

Q. How best can organisations be persuaded to adopt the principles of a new Code on a voluntary basis?

Q. Are there specific aspects of the proposed Code that should be made mandatory for all organisations?

6. FUTURE DEVELOPMENTS

The approach we have outlined here is designed to begin to bring order to what is a complex landscape, in a proportionate way. As such, it envisages a staged approach, addressing public space and public sector issues as a priority while establishing a set of principles with much wider potential application, including in the private sector and individual sphere.

This is not intended to be the last word in this area and this issue will be kept under review. The Code itself will be a living document which can be amended and extended as necessary, to reflect new standards or good practice.

It will also be necessary to keep abreast of new technological capabilities and developments and how these may be used by organisations in new ways. The challenge will be to ensure that they can be integrated into the established framework so that the potential for further increases in the level of unwarranted intrusion into private lives are identified at an early stage and addressed.

Finally, there is little regulation in this area in relation to the use of technology by private individuals. Again, the relative costs of such technology combined with innovative developments have seen increasing access to the use of such technology by private individuals. There has been a corresponding increase in concerns raised by other private individuals who feel that their own privacy is being compromised, for example by neighbours' security systems which may partially overlook boundaries. This is another complex area of conflicting needs, but one on which further specific provision may in due course be required. Views on this are welcomed.

Q. Is there a need to regulate the use of CCTV and similar systems by private individuals? What issues should be covered?

Q. Are there other surveillance camera technologies in operation or development for which guidance or legislation may be required?

Q. Are there any other matters on which new or further regulation may be required?

7. CONSULTATION CRITERIA

Where possible, the Consultation follows the Code of Practice on Consultation, the criteria for which are set out below:

Criterion 1 – When to consult – Formal consultation should take place at a stage when there is scope to influence the policy outcome.

Criterion 2 – Duration of consultation exercises – Consultations should normally last for at least 12 weeks with consideration given to longer timescales where feasible and sensible.

Criterion 3 – Clarity of scope and impact – Consultation documents should be clear about the consultation process, what is being proposed, the scope to influence and the expected costs and benefits of the proposals.

Criterion 4 – Accessibility of consultation exercises – Consultation exercises should be designed to be accessible to, and clearly targeted at, those people the exercise is intended to reach.

Criterion 5 – The burden of consultation – Keeping the burden of consultation to a minimum is essential if consultations are to be effective and if consultees' buy-in to the process is to be obtained.

Criterion 6 – Responsiveness of consultation exercises – Consultation responses should be analysed carefully and clear feedback should be provided to participants following the consultation.

Criterion 7 – Capacity to consult – Officials running consultations should seek guidance in how to run an effective consultation exercise and share what they have learned from the experience.

The full Code of Practice on Consultation is available at: http://www.berr.gov.uk/whatwedo/bre/consultation-guidance/page44420.html

7.1 CONSULTATION CO-ORDINATOR

If you have a complaint or comment about the Home Office's approach to consultation, you should contact the Home Office Consultation Co-ordinator, Adam McArdle at the address below. Please DO NOT send your response to this consultation to Adam McArdle. The Co-ordinator works to promote best practice standards set by the Code of Practice, advises policy teams on how to conduct consultations and investigates complaints made against the Home Office. He does not process your response to this consultation.

The Co-ordinator can be emailed at:

Adam.Mcardle2@homeoffice.gsi.gov.uk or alternatively write to him at:

Adam McArdle, Consultation Co-ordinator
Home Office
Performance and Programme Delivery
Home Office
3rd Floor - North West Quarter
Peel Building
2 Marsham Street
London
SW1P 4DF

ANNEX A - EXISTING PRIMARY LEGISLATION

DATA PROTECTION ACT 1998 (DPA)

The DPA applies to the processing of personal data by data controllers. Personal data includes data that can be used on its own, or in conjunction with other information likely to be in, or to come into, the possession of the same controller, to identify an individual. Operation of CCTV systems should therefore conform with the eight data protection principles, although there are some exemptions in the case of domestic use.

The Information Commissioner issued a CCTV Code of Practice (revised January 2008) in order to help ensure compliance with the DPA and transparency when processing personal data.

The Code provides good practice advice in order to:

- ensure that those capturing images of individuals comply with the DPA
- ensure that the images captured are useable and
- reassure those whose images are being captured

It refers to standards issued by the Home Office Scientific Development Branch for defining the operational requirements, technical requirements and system validation of a CCTV system.

The Information Commissioner regulates compliance with the DPA, but not the cameras themselves.

THE PRIVATE SECURITY INDUSTRY ACT (2001, SCOTLAND 2007)

The Security Industry Authority (SIA) is the organisation responsible for regulating the private security industry in the UK. A SIA licence is required for undertaking the licensable activities of a public space surveillance (CCTV) operative, and supplying services for the purposes of, or in connection with, any contract to a consumer. Such licences are required by security contractors. This means that if a local authority employs a private company to supply the CCTV operatives, all these operative need to have SIA licences. However if the operatives are employees of the local authority, they do not require a licence.

HUMAN RIGHTS ACT 1998

The European Convention on Human Rights (ECHR) Article 8 protects an individual's right to respect for a private and family life. Consequently where a CCTV system is operated by or on behalf of a public authority, the authority will also need to consider wider human rights issues and in particular the implications of ECHR Article 8. The Information Commissioner's CCTV Code of Practice also provides guidance on meeting this requirement.

CRIME AND DISORDER ACT 1998

The Crime and Disorder Act 1998 gave local authorities in England and Wales the responsibility to formulate and implement a strategy to reduce crime and disorder in their area. A key part to many of these strategies has been the installation and/or up grading of CCTV systems.

CRIMINAL JUSTICE AND PUBLIC ORDER ACT 1994

This Act creates the power for local authorities to provide CCTV coverage of any land within their area for the purpose of crime prevention or victim welfare.

POLICE AND CRIMINAL EVIDENCE ACT 1984

Codes of Practice issued under the Act detail how exhibits, such as CCTV images, used for investigations have to be handled so that they are admissible in court.

CRIMINAL PROCEDURES AND INVESTIGATIONS ACT 1996

This Act requires disclosure of video evidence to defendants.

REGULATION OF INVESTIGATORY POWERS ACT 2000

Covert CCTV surveillance is regulated under this Act by the Office of the Surveillance Commissioner. When an overt CCTV system is used to follow a specific, known individual in a planned operation, this has been classed as 'directed surveillance' and also comes under RIPA. (This consultation is not designed to address the question of covert usage - its primary purpose is designed to elicit views on the overt use of CCTV/ANPR in public or semi-public areas.)

TRANSPORT ACT 2000 AND TRAFFIC MANAGEMENT ACT 2004

These Acts require certification of equipment used for civil traffic enforcement devices such as CCTV to monitor bus lanes. Many local authorities use CCTV for traffic enforcement. The Acts are enforced by the Vehicle Certification Agency on behalf of the Secretary of State for Transport. The agency has published detailed Codes of practice for CCTV enforcement systems.

ISBN: 978-1-84987-433-5

HO_01763_G