

The Information Commissioner's response to the Home Office consultation on a code of practice relating to surveillance cameras

Introduction

The Information Commissioner has responsibility for promoting and enforcing the Data Protection Act 1998 (DPA) and the Freedom of Information Act 2000 (FOIA). He is independent from government and upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The Commissioner does this by providing guidance to individuals and organisations, solving problems where he can, and taking appropriate action where the law is broken. The Information Commissioner welcomes the opportunity to respond to the above consultation. In this response we shall focus on issues that have transparency, data protection and privacy implications.

Government approach to regulatory framework

The Information Commissioner is keen to see effective regulation of CCTV and automatic number plate recognition (ANPR) systems and other emerging camera technologies. Ensuring camera surveillance is subject to effective control is essential and the Commissioner supports government proposals to drive up standards and to regulate further in this important area. To help ensure CCTV cameras are used responsibly, the Information Commissioner published a CCTV code of practice in 2000, revised in 2008, to assist CCTV operators comply with data protection legislation http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/ico_cctvfinal_2301.pdf . The Data Protection Act 1998 (DPA) will still apply where images related to individuals are involved and across all sectors throughout the UK. It is important that the Home Secretary's surveillance camera code of practice is consistent with these requirements, enhances safeguards and does not lead to any confusion about legislative obligations.

In his evidence to the Public Bill Committee, the Information Commissioner emphasised that it would be important to clarify the roles of the existing and proposed commissioners who may have a regulatory interest in CCTV and ANPR because, if there were overlaps in responsibilities, there was a risk that commissioners could adopt differing interpretive approaches and guidance on each others' statutory provisions. It is very welcome, therefore, that the government has made it clear that nothing in the Protection of Freedoms Bill in relation to the regulation of surveillance camera systems will interfere with the current role and

responsibilities of the Information Commissioner and he will continue to have primacy and sole responsibility for data protection. This is a welcome clarification and it would be helpful to have this reflected in the code.

The Government has made it clear that the role and responsibilities of the new Surveillance Camera Commissioner will complement but be distinct from those of the Information Commissioner and there will be a strong degree of mutual interest. The Information Commissioner agrees that it is important that he works closely with the Surveillance Camera Commissioner. In order to have an effective, transparent and consistent regulatory framework, it is essential that all the commissioners who have a role in overseeing camera surveillance have clear and complementary roles.

The consultation document says the Surveillance Camera Code will draw on relevant good practice guidance such as that developed by the Information Commissioner. It is worth clarifying that the Information Commissioner's CCTV Code of Practice is intended to help CCTV operators comply with their legal obligations and is not just aimed at the virtuous who want to adopt best practice. It sets out the Information Commissioner's recommendations on how the legal requirements of the Data Protection Act can be met and these are based on the legally enforceable data protection principles. As the Information Commissioner's code makes clear, operators may use alternative methods to meet these legal requirements but if they do nothing, they risk breaking the law.

It may be helpful for the government to consider whether the Home Secretary's code should be aimed primarily at setting standards for technical and operational issues. It would be possible for the code to make reference to the Information Commissioner's code - which in turn could be amended to cross reference with the Home Secretary's code, as our current code does with the guidelines provided by the Home Office's Scientific Development Branch (HOSDB). Since both codes will have to co-exist, it is important they are complementary and not contradictory. Enforcing data protection requirements will engage the Information Commissioner's supervisory functions so it is essential that there are no misunderstandings on the part of those who have to comply with the law.

Purpose of the code

It is important that the government is clear about the purpose of the surveillance camera code. The Ministerial foreword highlights the dramatic growth in volume and capability of surveillance technologies and its determination that significant increases in state surveillance should not go unchecked. But it also emphasises that the government does not intend that anything in their proposals should hamper the ability of the law enforcement agencies or others to use such technology as necessary

to prevent or detect crime, or help to ensure the safety and security of individuals. It is not always clear in the consultation document how the government intends to balance the aims of driving up standards and the efficiency of surveillance camera systems with those of ensuring such systems are necessary, proportionate and justified. While these aims are not necessarily mutually exclusive, at times the main thrust of the consultation document appears to be aimed at getting the most out of surveillance cameras rather than identifying ways of meeting some of the privacy challenges outlined in the foreword and background chapter.

Background

The examples of CCTV and ANPR systems described in the background chapter show the breadth and depth of surveillance camera usage by both the public and private sectors. The consultation document recognises the blended nature of CCTV usage by different organisations but these uses do not always appear to be reflected in the proposed coverage of the code. The Information Commissioner is concerned that only the police and local government will be obliged to “have regard to” the proposed code, at least initially. This could cause problems in practice given the many partnership arrangements between the public and private sectors for town centre monitoring and the increasing use of shared common infrastructures particularly in the public sector.

There is also widespread use of CCTV and ANPR systems across all sectors including government agencies and the increasing deployment of ANPR in the private sector such as with car park operation, where sometimes details of people’s vehicle movements are stored indefinitely and insufficient safeguards are in place regarding security, access and further use. The Information Commissioner considers further thought should be given to the implications of limiting the application of the code to the police and local government only and adopting a cautious incremental approach. At the very least, the government should consider extending the scope to central government department and agencies, especially those with significant usage or involvement with camera systems such as the Department for Transport; DVLA; Highways Agency; Home Office; UKBA; SOCA; and other law enforcement agencies.

The background chapter highlights the benefits of CCTV and ANPR systems for the purposes of crime prevention and detection, public safety and traffic management. It does not address the use of surveillance cameras for commercial purposes such as car parking; marketing and promotion; or income generation. While the citizen may expect the intrusion of surveillance cameras for crime and safety purposes, complaints to this office show that they are less supportive of cameras being used for wider commercial purposes.

The background chapter says that 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. We are aware that private car parking organisations are building up large collections of ANPR “read” data and sometimes are retaining the data indefinitely. Clearly some information on these databases can be a valuable resource for police forces investigating crimes but use of this information must comply with the requirements of the Data Protection Act. The Information Commissioner has concerns that some of the purposes for which this information is being used appear to go way beyond the original justification for collecting the data in the first place, usually to enforce ‘short stay’ and other parking restrictions, and lengthy or indefinite retention of all ANPR data reads is inappropriate for managing a car park.

The section 29 exemption to the DPA permits the disclosure of ANPR data to the police where if not releasing it would be likely to prejudice any attempt by police to prevent or detect a crime, or capture and prosecute a suspect. The Information Commissioner’s Office has worked closely with ACPO and a police force to establish and test whether private sector ANPR data can be shared in a proportionate and less privacy intrusive way at locations where there are pressing reasons for the police to be able to access this data. We also recognise its use in covert surveillance, for example, the police have real time access to all ANPR reads from Transport for London’s congestion charging cameras allowing them to track all vehicles entering central London. A certificate issued by the Home Secretary under Section 28 (national security) of the DPA exempts the police from some DPA provisions, to the extent to which compliance affects national security considerations. Under the terms of this certificate, the Commissioner of the Metropolitan Police Service is required to provide an annual report to the Information Commissioner so that he can be satisfied that the personal information processed under the certificate is required for the purposes of safeguarding national security and that any processing that is undertaken, other than under an exemption set out in the certificate, is carried out in compliance with the Data Protection Act 1998.

We are concerned, however, about the police being offered routine and unlimited access to information about every vehicle, for example, entering and exiting retail and fast food outlet car parks, regardless of whether the vehicles are of interest to the police. We also have concerns about the accuracy of this data and the potential for misreads if private sector cameras are positioned incorrectly or used in adverse conditions. There are also wider security concerns about private organisations sharing police information about “vehicles of interest” without sufficient security and contractual arrangements in place. We also have some enduring concerns that ANPR data is not always subject to proper information governance,

particularly in the private sector, and that insufficient safeguards are in place to ensure the information is kept securely and operators check that vehicle keeper records that are relied upon are accurate and up to date. We are looking to provide more guidance for ANPR system operators and ANPR data users on how to comply with their obligations under data protection and human rights legislation. It would be helpful if the Home Secretary's code and the Surveillance Camera Commissioner could address these technical and operational issues.

Allowing police unlimited access to all private sector ANPR databases would represent a significant extension of surveillance capability and we have made it clear that we would be concerned if such a pervasive ANPR network was rolled out without appropriate debate, consultation and if appropriate, clear legislative safeguards. The previous Government acknowledged that bulk ANPR data sharing should be "subject to a robust regulatory regime that ensures reasonable transparency and scrutiny" (Tony Mc Nulty's, then Minister of State for Security, Counter-terrorism, Crime and Policing, statement to Parliament 17 July 2007).

We have welcomed Government plans to regulate the use of ANPR and made it clear that we would not want to see any tightening of ANPR regulation to be restricted to the police but would want to see it extended to wider public authorities and the private sector. In the absence of a statutory basis for unlimited police use and mass sharing of private sector ANPR data, we shall be reminding the parties involved that they must be able to justify collection and sharing of ANPR data in each particular case. We shall continue to advise the police that any proposals to share third parties' ANPR data should be based on a pressing need and must be subject to adequate safeguards. It will be important to ensure that the Home Secretary's code and the approach of the Camera Surveillance Commissioner are aligned with this work.

Format of the code

The Information Commissioner's CCTV code is written from the perspective of the CCTV operator, which we have learned from consultation with camera system operators and past experience is a more helpful and practical approach than trying to produce a high level document aimed at a wide range of audiences. It may be helpful to provide separate companion documents for individuals and small businesses who may be affected by aspects of the code. The Commissioner has adopted this approach with some the codes he has issued under his powers.

Contents

i. Pre-planning

The Information Commissioner welcomes the emphasis in the consultation document on the importance of ensuring proportionality of use of surveillance cameras at the pre-planning stage and the proposal that anyone considering the use of surveillance cameras should undertake a thorough assessment of the purpose, likely value and wider impact before proceeding. The Commissioner advocates considering the use of Privacy Impact Assessments and has published a handbook which includes assessment criteria (see link below). We support the use of similar checklists to help organisations address the right questions.

http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/index.html

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

Other preparatory checks could include an assessment of the long-term sustainability of the system. Having the resources for the initial capital costs but insufficient funding to ensure effective operation of the system, including maintenance and replacement of devices, could engage concerns about data protection compliance on issues such as image quality and security. Reviews should include assessments of reliability and accuracy of more proactive technologies or enabling software such as ANPR and facial recognition. When an organisation is planning to use an ANPR system, they need to look at the quality of the hotlists. The whole system has to be examined and measures put in place to keep it up to date.

It would be helpful to have a checklist to help organisations assess whether covert but non-directed surveillance is justified and proportionate. The code could have a link to the Information Commissioner's guidance on privacy impact assessments.

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

The Commissioner's current CCTV code of practice provides advice on the following of good practice and its provisions are relevant. A key feature of data protection legislation is the use of "necessity tests" which provide a framework for deciding whether the processing of people's personal information is necessary for the purpose, as well as being fair and lawful which includes addressing Human Right Act requirements.

Guidance on this is included in the Information Commissioner's CCTV Code of Practice. The code is primarily aimed at helping CCTV operators comply with the legal duties of the Data Protection Act and Human Rights Act but it also includes good practice advice which is built into compliance recommendations. Other Information Commissioner's Office publications

that may be useful include our codes of practice on data sharing and privacy notices, and our privacy impact assessment handbook. The European Forum for Urban Security's "Charter for democratic use of video-surveillance" also provides useful advice for carrying out prior audits to define local needs objectively and consider necessity, proportionality and justification considerations. ACPO's ANPR guidelines would be a useful starting point for developing guidance on ANPR.

ii. Standards

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

Some of the most challenging and longstanding problems with CCTV systems have included poor image quality; the technical difficulties and cost of police retrieval of digital images from a wide variety of incompatible systems; technical and organisational barriers to organisations sharing images, for example between police and prosecutors; and the criminal justice system being unable to use CCTV footage as evidence.

The new code will provide a renewed opportunity to set out new technical standards in these areas. It would be helpful to establish a common technical standards baseline, especially for developing technologies. Clearly defining standards to be adopted in the implementation of new systems may not pose the same challenges as applying these to existing systems. Any requirements should be clear about their application and timescales for compliance.

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

The development of standards relating to the accuracy and reliability of facial recognition, ANPR and other video analytics systems would be very helpful. These should include the adequacy of the databases underpinning these camera surveillance systems, in order to minimise the number of false positives. The Information Commissioner would welcome government efforts to ensure that the DVLA and Motor Insurance databases are as accurate and up to date as possible if they are to be used to support ANPR systems. It would also be helpful to have standards that incorporate "Privacy by Design" features into camera systems that would facilitate easy subject access and privacy friendly solutions such as software to enable images of third parties to be blurred.

Standards relating to the security of CCTV systems and images would also be very valuable, particularly in relation to portable media, wireless and internet systems. The Information Commissioner has made it clear that organisations must have a properly managed approach to risk and we

advise organisations to undertake a review to identify any data protection weaknesses, particularly the risk of theft or loss of unencrypted laptops and portable media storage devices containing potentially sensitive evidential footage of an incident which if lost could be damaging or distressing to a victim or witness.

The Information Commissioner recognises that encryption is not always straightforward for CCTV cameras and systems and has acknowledged that it can cause some practical difficulties for the police when downloading from different systems and, if available at all, may be ineffective. Many existing CCTV systems are not encrypted and the Home Office Scientific Development Branch (HOSDB) have advised us that encryption would not be possible for older systems based on VHS tape recording, and encryption can be difficult with digital recording systems. They have also advised us that they have concerns that various manufacturers claim their equipment is encrypted, when actually it is not to any recognised standard.

Our data protection advice is that if encryption is not possible because of the technology limitations or evidential requirements, then organisations need to put alternative, robust, security measures in place to guard against unauthorised use or disclosure. It was always intended that the Information Commissioner's Office would continue to look at some of the technical and management issues concerning security of CCTV images with HOSDB and the National CCTV Strategy Board standards subgroup. However, this workstream ceased when the Interim CCTV Regulator was appointed given his role. This area still needs addressing and we would wish to participate in further work with CCTV operators, the police and the Surveillance Camera Commissioner.

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

It will be difficult to achieve consistency without developing detailed technical specifications. Under data protection legislation, the quality of camera images should be adequate for their purpose. We have supported initiatives by the National CCTV Strategy Board, the Interim CCTV regulator and the HOSDB to improve standards and support the government's plans to drive up technical standards where this will assist with data protection compliance.

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

The main drawback is that rapidly developing technologies, and the novel uses to which they are put, can overtake any common technical standards, especially if such standards take a long time to be agreed. It may be helpful to adopt a flexible approach similar to that of the seventh

principle of the DPA on information security. This says that organisations' assessment of appropriate security measures should consider technological developments and the costs involved. The DPA does not require organisations to have cutting edge security technology to protect personal data but in order to comply with the Act, organisations need to have appropriate security safeguards based upon risk to individuals and should regularly review their security as technology advances and risks change. The Surveillance Camera Commissioner could provide a valuable role in keeping abreast of new technologies and in ensuring that new standards are approved when appropriate.

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

It would be helpful to develop a common approach to undertaking privacy impact assessments perhaps, for example, by producing bespoke sectoral impact assessments. It may also be helpful to develop non-technical standards relating to privacy friendly approaches such as ensuring cameras do not overlook private property; ways of facilitating subject access requests under the DPA; and the siting of cameras in areas where people have a high expectation of privacy such as in toilets and changing rooms.

Many larger organisations have CCTV policies but these are of varying quality and often out of date. It may be helpful to produce a model or outline CCTV policy which would help organisations articulate their own approach to issues such as governance of the system, who can view or access the data, security arrangements, signage, disclosure of information, and staff training/accreditation.

Data Protection

The Information Commissioner is clear that there cannot be a lessening of legal compliance with the requirements of the DPA and HRA or any regulatory actions the Commissioner may wish to take in relation to surveillance camera usage. The Information Commissioner welcomes the provision in the Protection of Freedoms Bill that he must be consulted by the Secretary of State in the course of preparing the code. As the UK's independent authority on upholding information rights, the Information Commissioner is keen to ensure the provisions of the code are consistent with and complement existing data protection safeguards and do not lead to any confusion over what regulatory requirements apply in practice. This is particularly true in relation to the Information Commissioner's own existing published CCTV code of practice which helps organisations comply with the legal requirements of the DPA and adopt good practice standards.

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?

Clearly the Secretary of State's code has to address legal compliance issues especially those arising from the DPA, Regulation of Investigatory Powers Act 2000 (RIPA) and the Human Rights Act (HRA) but given the limitations of its statutory authority, it is difficult to see how it could subsume the Information Commissioner's existing code when it will not have the same geographic or sectoral coverage. It is essential that surveillance camera operators understand that they must comply with the legally enforceable provisions of the DPA even though they may not be obliged to follow the Secretary of State's code.

The Information Commissioner welcomes the requirement to be consulted by the Secretary of State on the provisions of the proposed code and he will use this opportunity to try to ensure they reflect the requirements of existing data protection law. But it may be unrealistic to expect to reconcile different legislative approaches within one document, especially where there are differences in territorial scope, sectors covered, compliance obligations and enforcement mechanisms. In addition the Information Commissioner is able to deal with matters that relate to data generated or used particularly in connection with ANPR where existing databases are consulted and where vehicle movement details are recorded in databases for future use. The development of automatic facial recognition will also engage similar issues of ensuring appropriate supervision of all personal data in closely related contexts. The Information Commissioner would not want to see any weakening of data protection safeguards but wants to help ensure that any new arrangements enhance the work the Information Commissioner has done already in setting good practice data handling standards for CCTV and ANPR system operators.

Individuals must also be clear about how to exercise their rights in relation to the DPA, for example their right to request to view and have copies of images of themselves. Some of the most complex CCTV cases we deal with involve wider disputes between employers and employees or between detainees and the police or immigration services. The Information Commissioner's advisers and caseworkers have to answer queries and consider complaints on a range of data protection and freedom of information issues related to CCTV, including rights of subject access, whether third party images have to be blurred or obscured, often taking account of rules relating to disciplinary or legal proceedings. The Information Commissioner has to consider complaints under Section 42 of the Data Protection Act and, as the law stands, it is difficult to see how the Home Secretary's code or the Surveillance Camera Commissioner could

offer up to date advice on such issues, especially as only the Information Commissioner can make formal assessments on compliance with data protection legislation.

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

If the Surveillance Camera Code is to include guidance on these issues, the standards cannot be any less than the legal requirements of the Data Protection Act, nor should it contradict good practice recommendations included in the Information Commissioner's CCTV code of practice or in any other guidance such as our statutory data sharing code. The Home Secretary's code could make reference to the Information Commissioner's code - which in turn could be amended to cross reference with the Home Secretary's code. It is important that the codes are complementary and not contradictory, and do not lead to misunderstandings on the part of those who have to comply with data protection law.

The consultation document says that it may be particularly helpful for the new code to provide further or refined guidance on data retention periods, especially in respect of ANPR data. The Information Commissioner recognises that ANPR is a useful tool for law enforcement agencies and we have worked closely with ACPO, the NPIA and some individual police forces to ensure their use of ANPR complies with the data protection principles. Initially, police ANPR systems did not have a deletion function but following recommendations from the Information Commissioner, the police have been rolling out software to local forces to ensure that ANPR data is deleted after two years, unless required for investigative or evidential purposes. This work is now complete and all forces now have weeding functionality for ANPR data. This has so far resulted in the deletion of tens of millions of records of people's car journeys that are not of interest to the police. The Information Commissioner believes that the new retention rules represent a far more proportionate approach to retaining ANPR data. However, we recognise that the functionality of the police ANPR system is continuing to develop and have agreed with ACPO that retention periods should be kept under review in the light of evidence of the usefulness of older records for counter terrorism purposes.

We have also worked with the police on tightening up access controls to the National ANPR Data Centre and making efforts to improve the accuracy of hotlists. Much of the detailed work on guidelines, memoranda of understanding and privacy friendly technical solutions has been undertaken by the NPIA and we are concerned about how this level of information governance will continue to be provided when the NPIA is abolished. The Home Secretary's code could have an important role to play in helping ensure that detailed rules for the use of CCTV and ANPR by

the police are established and maintained if the NPJA is no longer available to help undertake the role.

Given that the code, at least initially, will apply primarily to local authorities and the police, an area of common confusion is the extent to which RIPA applies to covert surveillance. It may be helpful if the code provided broad advice on this, linked to the guidance of the Office of the Surveillance Commissioner.

It may also be useful to provide further or refined guidance on data sharing provisions, especially between the police and local authorities where they share information in CCTV control centres. These would need to be aligned with other provisions such as the Information Commissioner's statutory data sharing code and the provisions of the crime and justice legislation.

Provision of information

The consultation document refers to the development and publication of effective complaints procedures for existing schemes and says these would be an important way of addressing public concerns about proportionality of use and data security. If personal information is involved, then any complaints not resolved at a local level may ultimately be directed towards the Information Commissioner's Office where questions of compliance with the DPA are engaged as the Commissioner is bound to make an assessment of compliance with its provisions in such circumstances.

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

The Information Commissioner encourages transparency about surveillance systems wherever possible, whilst recognising that there may be specific circumstances where disclosing the exact location of individual cameras would be likely to prejudice the prevention and detection of crime or the apprehension and prosecution of offenders. It is clear from data protection and freedom of information complaints to the Information Commissioner that too often people do not know which organisations are operating the cameras and for what purpose and this undermines public trust and confidence in camera surveillance.

The general standard in the DPA is that 'fair processing information' – including the identity of the organisation collecting the information and the purpose/s it will be used for – must be provided at the time the data controller first collects the data. There is an argument, therefore, that camera operators should provide signage or some other form of notification at the time the image is captured and therefore at the place it is captured. However, we are mindful of both the risk of prejudice in this

approach and the logistical problems, including the risk of distracting drivers, of providing extensive fair processing information at each and every camera site.

Since traditional ways of providing fair processing information at the point of collection may not always work well with camera systems, particularly on the road network, we have encouraged organisations to think of other ways information can be provided, backed up by subsidiary supporting information on websites. Informing people about other camera uses are more challenging, such as body worn devices, national ANPR or CCTV networks or where new, proactive technologies are used such as facial recognition systems. There is also the challenge of providing information where the police want to share camera infrastructures or furniture with the Highways Agency, local transport authorities or local councils.

The Information Commissioner does have specific concerns about the lack of transparency surrounding the collection of ANPR data and believes that the government should consider developing a national communication strategy aimed at improving public levels of awareness on camera usage on our highways. At a national level the government could set up a national cameras webpage on Directgov. There appears to be a growing view amongst motorists that ANPR cameras are being introduced and positioned in order to generate income rather than to prevent or detect crime, improve public safety or manage and enforce traffic and parking restrictions; and the lack of signage or information is helping to reinforce this view. We think that providing more detailed information to the public will help to address the general lack of public awareness about ANPR cameras. We are very keen to try to arrive at an acceptable national solution to this issue, being mindful of any relevant decisions by the courts and tribunals on FOI requests, to ensure that a consistently high approach to DPA compliance is adopted whilst at the same time recognising logistical difficulties and realising any economies of scale.

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

The Information Commissioner's CCTV code of practice provides some good practice examples but these could be refined further. The Information Commissioner recognises that there can be practical difficulties when providing detailed information though signage on the highway and more conventional DPA fair processing requirements can be difficult to comply with where personal data is collected through cameras. The Information Commissioner has provided advice that he does not expect every individual CCTV or ANPR camera on the highway to be signed in order for the processing of personal information to be fair. However, he does expect organisations to make people aware that they are entering an area covered by cameras and to provide them with certain

information relating to their use. The Information Commissioner advises that clear and prominent signage at the perimeter of areas covered by ANPR and CCTV roadside cameras, and further signage to reinforce this within each area, would seem to be the most straightforward way of communicating initial fair processing information to individuals prior to, and at the point at which, their personal information is collected.

The Information Commissioner has also advised the police to improve transparency on their use of ANPR cameras for overt policing. The ACPO lead of the police's ANPR National User Group has encouraged police forces to provide ANPR signage on police liveried vehicles and he has used roadside variable matrix signs to publicise the use of roadside ANPR cameras.

In some cases, such as where specific operations are being carried out, some more specific, additional 'fair processing information' may be necessary. For example, the Information Commissioner has advised organisations that they create a page on their website with a supporting layered privacy notice specific to ANPR operations. We have also advised organisations to consider providing a hard copy of this information for people who do not have access to the internet but would like further information. For more information about layered privacy notices please see our Privacy Notices Code of Practice:

http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/privacy_notices_cop_final.pdf

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

It would be helpful if the code also addressed the use of surveillance cameras for commercial purposes such as car parking; marketing and promotion; or income generation. For example, some organisations are looking to exploit ANPR data commercially by offering it for sale for market research purposes or identifying "vehicles of interest" to other organisations. There is also anecdotal evidence that some car park operators and bailiffs are misusing ANPR systems in order to generate more income, for example when drivers are unaware of private car parking restrictions through lack of effective signage, or organisations do not take sufficient care to ensure vehicle keeper data information is accurate and kept up to date. Some organisations are also using facial recognition and ANPR technologies to track and analyse customers' behaviour for example to measure footfall, observe traffic flows around stores/shopping centres and study the impact of marketing initiatives. While the citizen may expect the intrusion of surveillance cameras for crime and safety purposes, complaints to this office show that they are far less supportive of cameras being used for wider commercial purposes.

Implementation

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

In the absence of an underpinning enforcement regime, the government should identify important drivers and ensure they are made as effective as possible. For example, public funding decisions could be made dependent on adherence to the code's principles, especially where public money was spent on new initiatives or upgrading existing systems.

Although the Home Secretary's code of practice is not mandatory, where its recommendations intersect with data protection law it may be helpful to remind organisations that the Information Commissioner has powers to handle complaints and take enforcement action concerning breaches of the DPA.

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

As the government recognises, a baseline of mandatory requirements already exists around the use of surveillance cameras for example: through the Data Protection Act when personal data is processed; through RIPA when cameras are used for intrusive or directed covert surveillance; when Article 8 of the Human Rights Act is engaged; or when people make requests for information under the Freedom of Information Act.

It appears that there is nothing in the Protection of Freedoms Bill that gives the Secretary of State the power to make further aspects of the Surveillance Camera code mandatory. There is also no mechanism in the Bill for direct enforcement of the code or for dealing with individual complaints about non compliance with the code. It is not clear from the consultation document whether more primary legislation is contemplated to make further aspects mandatory.

The Information Commissioner is concerned that only the police and local government will be obliged to "have regard" to the proposed code, at least initially. This could cause problems in practice given the many partnership arrangements between the public and private sectors for town centre monitoring. There is also widespread use of CCTV and ANPR systems across all sectors including government agencies and increasing deployment of ANPR in the private sector such as with car park operation, where sometimes details of people's vehicle movements are stored indefinitely and insufficient safeguards are in place regarding security, access and further use. The Information Commissioner considers further

thought should be given to the implications of limiting the application of the code to the police and local government only.

Future developments

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

The Information Commissioner recognises that there is increasing public concern about domestic use of CCTV systems, such as use by neighbours. As CCTV and surveillance equipment becomes more affordable and readily available, the Commissioner receives more calls relating to its use by private individuals. But in practical terms domestic use of CCTV is largely exempt from the requirements of the DPA and this is made clear in the Information Commissioner's CCTV code of practice. This means that where CCTV is put on a residential property by an individual for limited purposes, such as protecting their property from burglary, then it is exempt from the data protection principles and householders do not have to register with the Information Commissioner's Office.

Although the DPA provisions are unlikely to apply to individuals who install CCTV on their properties for their own purposes, other legislation may do so. For example, planning law can be relevant to the siting of cameras and criminal law may apply depending on how the collected images are used. If the CCTV images are used for voyeuristic purposes, harassment, anti social behaviour or other matters dealt with under the criminal law, then these are matters for the police to investigate.

It would appear to be a big jump from regulating the use of CCTV by police and local authorities to regulating the use of such systems by individuals. Initially, it may be better to focus on extending the legislation to central government departments and agencies, especially the Highways Agency and the DVLA; public transport providers such as Transport for London; and private organisations surveillance of public spaces, rather than individuals' use of CCTV cameras.

Given the focus of the Home Secretary's code of practice and the Protection of Freedoms Bill is very much on the State's intrusion into the lives of individuals, it may be difficult to address domestic use of CCTV in the Surveillance Camera Code. The government could helpfully provide guidelines for householders to follow but it may be better to include these in a separate leaflet for individuals rather than in a code primarily aimed at improving standards for the use of surveillance camera systems used by the police and local authorities.

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

The Information Commissioner would support the setting of standards for new and developing technologies, especially where there is still an opportunity to make a difference, for example with facial recognition and other video analytics technologies. With a lowering cost base it is increasingly feasible for organisations to use such technologies but there are questions about their reliability, and the accuracy of the hotlists that underpin them. Appropriate technical standards may help but it is also important that organisations are aware that it is not enough to rely on automatic processing and that safeguards must be put in place to deal with false positives and people's complaints where they think they have been wrongly identified by such technologies.

The European Commission has published a Communication on its strategy for modernising the EU legal system for the protection of personal data. The communication indicates that the concept of Privacy by Design is likely to be a feature of any future European data protection legislation, as is an obligation for data controllers to carry out data protection impact assessments in specific cases. This highlights the importance of organisations adopting privacy friendly features from the very start and guidance on this would be very helpful.

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

These matters have been referred to in our earlier comments, particularly in reference to the scope of the current proposals and the development of technologies such as facial recognition and other video analytic systems.

Existing Primary legislation Annex A

In addition, the Information Commissioner regulates compliance with the Freedom of Information Act 2000; and under the "lawfulness" principle of the Data Protection Act 1998 has to take into account Human Rights Act considerations.

24 May 2011