States of Jersey
States Assembly

États de Jersey
Assemblée des États

Education and Home Affairs Scrutiny Panel

Camera Surveillance in Jersey

Presented to the States on 16th January 2014

SR1/2014

Contents

1. Chairman's Foreword

This has been an interesting review and deals with a topic which some may question the need for scrutiny. After all, a camera is a camera. However, since cameras were first introduced on the streets of St Helier, in 1995/6, the world has moved on. Whilst the needs and perception of society for protection may remain the same, the requirement for moral accountability has moved on significantly. Transparency and the ability to justify the use of CCTV systems and, of course, expenditure, are far more important now than ever before.

Issues relating to Data Protection must now be taken seriously. Failure to comply with legislation has been shown in the Royal Court to have severe consequences. The pressure will only increase as we head towards the introduction of Freedom of Information legislation. Again, failure to comply will have criminal implications.

Our report reveals, amongst numerous other points, that the Police have not been keeping records which evidence the continued need for public surveillance cameras. Evidence of the value they provide for the public of the Island, the impact they have on the detection and prevention of crime or indeed on the prosecution of offenders tends to be little more than anecdotal. Firm evidence could be gained by continued monitoring and recording by operators and would provide the hugely important evidence needed to support a transparent approach to the needs of today's society. The lack of statistical evidence plays into the hands of opponents of CCTV surveillance and could, in the extreme, provide the grounds for funding to be withheld at some point in the future. Work done as long ago as 2006 cannot provide evidence of today's attitudes. Consent for surveillance is so important to our community and must be safeguarded. Surveillance by consent cannot be supported by conceptual or anecdotal evidence. In today's society, it must be backed by statistics and robust, firm evidence.

There are three important developments in CCTV use in Jersey which are being led by the States of Jersey Police, namely the introduction of body worn cameras for police officers, the proposal for a fixed Automatic Number Plate Recognition (ANPR) camera surveillance system around St Helier and the renewal and digitalisation of the Town Centre CCTV network. We examine each of these in detail in our report.

The announcement by the Police, just before we finalised our report, that they planned to extend body worn video cameras to all police officers on the beat was made without any

reference to the Scrutiny Panel. Whilst we believe that the processes and procedures around body worn cameras are quite robust it was of some concern to us that the Police should ignore our involvement and interest in this matter. This demonstrates a worrying lack of regard for political accountability on behalf of the Police

The proposal for fixed ANPR around St Helier is another sensitive matter. When Police in the UK attempted to install a similar system in the Hertfordshire town of Royston, it was declared illegal by the Information Commissioner on the grounds that it was excessive and out of proportion to the crime levels in that area. We believe that if such a system is to be proposed in Jersey there must be an informed public debate and political approval by the States before it is implemented.

The third key development, the extension and digitalisation of the Town Centre CCCTV network in St Helier, is not opposed by the Panel. We acknowledge its importance but point out that the new system gives the Police potentially very substantial additional powers of mass surveillance which need to be transparent if they are to be acceptable.

Public engagement must be the key, which to date has not been taken seriously enough by the States of Jersey Police in its handling of CCTV. Our report discusses methods available for evidencing public opinion, evidencing that public surveillance in Jersey is by consent. This is a recommendation that the Panel feels strongly about. The response from the Jersey Police at the draft stage of this report has been very positive, leaving me confident that the final recommendations relating to the Police could be implemented.

CCTV in private residences is becoming more prolific and along with that are the complaints about the invasion of privacy. The Panel recognises that this is a difficult nut to crack and one that currently falls between the legislative cracks in Jersey. However, there may be a solution. The Panel recommends that the Planning Minister gives serious consideration to reviewing the classification of CCTV as ‘permitted development’.

I can understand that looking at the recommendations contained in this report could lead the reader to think that the Panel is anti-Big Brother. This review is not about the feelings of the Panel Members. It is about the evidence. The evidence established by the Panel shows that the provision for the control of CCTV, particularly by the States of Jersey Police and the Data

Protection Commission is in need of updating to meet modern requirements in areas of transparency, responsibility and accountability.

The intention of this report is to wake States departments up to the need to improve compliance with current Data Protection requirements and to move towards ‘best practice’ in the field of CCTV surveillance. The Panel recognises that there is a resources requirement in the rectification of these issues, most particularly in the Data Protection Commission, this is an associated cost that must be met in preparation for the introduction of Freedom of Information legislation in 2015.

Before closing I wish to place on record the Panel’s appreciation of the contribution to the review made by our two advisers, Professor William Webster of the University of Stirling and Professor Peter Fussey of the University of Essex. Both provided a broad knowledge of the use and capabilities of modern surveillance systems in the UK and internationally and have helped to guide us in the provision of constructive recommendations to bring local governance arrangements up to date.

Deputy Jeremy Maçon

Chairman, Education and Home Affairs Scrutiny Panel

2. Panel Membership

Deputy Jeremy Maçon, Chairman

Connétable Michel Le Troquer

Deputy Geoffrey Southern

Deputy Montfort Tadier

3. Panel advisers

Professor William Webster, University of Stirling, is one of the founding directors of the Centre for Research into Information, Surveillance and Privacy (Crisp) is also Chair of the Living in Surveillance Societies (LiSS). He is a leading authority on the policies and practices surrounding the provision of closed circuit television/video surveillance cameras and systems in public places.

Professor Peter Fussey is professor of sociology at the University of Essex. He is a criminologist specializing in a number of areas including terrorism and counter-terrorism, major-event security, surveillance and society, organized crime and urban sociology.

4. Terms of Reference

The Education and Home Affairs Scrutiny Panel has agreed to undertake a review relating to the increasing prevalence of camera surveillance in the Island. The review will seek to ensure that the use of camera surveillance is reasonable, justifiable and transparent so that Islanders feel properly informed about and are able to support the security measures that are in place. The Panel will:

- Consider the scale of usage of camera surveillance in Jersey by the States of Jersey, commercial and non-commercial agencies
- Explore the role played by camera surveillance in policing, community safety, transport and in the criminal justice system
- Examine evidence for the effectiveness of camera surveillance in preventing and detecting crime and promoting public safety
- Explore public awareness of camera surveillance in Jersey
- Consider any concerns relating to the extent and purpose of intrusion into people's lives
- Establish the effectiveness of current guidelines/voluntary codes of best practice and their operation
- Establish the rights of access to information and camera footage by citizens and what rights employees have in relation to camera surveillance by their employers.
- Consider whether there is a need to develop the formal regulation of the use of camera surveillance.

The Panel will consult stakeholders and the public on what information should be available to any individual wishing to know more about overt surveillance cameras and how this information should be made available. The Panel will report its findings to the States

Further explanatory note: The review will be concerned with the overt use of systems such as CCTV and ANPR (Automated Number Plate Recognition) in public and semi-public places where people can generally see a camera, or are informed about its presence. It will not deal with covert surveillance techniques which are legislated for through the Regulation of Investigatory Powers (Jersey) Law 2005.

5. Key Findings

Paragraph numbers refer to Key Findings and Recommendations

Introduction:

The Scrutiny Panel believes that the public in Jersey deserves to have confidence that the use of camera surveillance is in the 'public interest'. This is especially the case for the Town Centre CCTV system operated by the States of Jersey Police. Public support for CCTV can be enhanced through the introduction of improved governance arrangements, including the introduction of a publicly available Code of Practice for the Town Centre CCTV system, performance audit and public engagement. The overall aim of the recommendations in this Scrutiny review then is to promote public awareness and debate about the capabilities of the various systems in use in the Island.

General principles:

Surveillance by consent: 'Surveillance by consent' is becoming a key element of CCTV practice in the UK and EU, especially in relation to the provision of public space systems in town and city centres. We have not encountered any initiatives that seek to understand the extent to which surveillance operates on a consensual basis in Jersey. Jersey's Data Protection Code of Practice should contain a statement on the need to seek consent from the people surveilled, including signs for public and private spaces and the need for consultation exercises for public camera installations. The Code should also contain a requirement to make the public aware of the purpose(s) of CCTV cameras and the location of cameras (paragraph 215 and advisers report section 2.1).

Proportionality: As a general principle, public service providers should take an evidence-based approach to the deployment of their camera systems. This should comprise an unambiguous statement of what the surveillance equipment is intended to achieve, a clear and evidenced identification of the type and prevalence of the issue it is intended to address, identification of non-intrusive alternative strategies, and consideration of whether such less intrusive measures could be deployed for those ends (and only discounted if inadequate). New efficacy monitoring processes should also be drawn upon to make an objective and informed evidence-based decision over whether surveillance cameras provide the most effective response to the particular issue. Experience of practices in the UK and other EU

countries could also be drawn on to inform this process. (see advisers' report: section 2.3 and recommendation 3)

Public attitudes: Public sector CCTV is generally perceived as benign, an anti-crime measure which brings few disadvantages of which people are conscious. CCTV in public spaces is not thought to intrude on personal privacy, a concept associated with the home. However, there is no real evidence that the public have a good understanding of the technological capabilities of CCTV systems or how they are used (paragraph 109).

Public engagement In order to retain public confidence in the appropriate use of CCTV in public spaces it is essential that the States of Jersey Police and other public sector CCTV operators engage with the public in an open and transparent way to explain the capabilities and limitations of their systems. The States of Jersey Police currently provide minimal information to the public on the Town Centre CCTV system, the location of cameras and its operational procedures. Performance reporting which used to be included in States of Jersey Police Annual reports has been discontinued. The introduction of a new Town Centre CCTV system sharpens the focus on the need for the States of Jersey Police to provide the public with a good business case demonstrating value for money for the project (paragraphs 127 & 167).

Evaluating the effectiveness of CCTV: There is an overwhelming view among operators that CCTV provides a vital function in enhancing public safety and reducing crime and disorder in Jersey, but robust evidence, backed by statistical data, for the reduction and prevention of crime is hard to find. Systems which do not achieve their stated purpose should be discontinued; however, we have seen no evidence that any such decisions have been taken in the public sector. The requirement that public sector CCTV operators should undertake a minimum standard of evaluation on an annual basis to ensure that their systems are effective and appropriately sited must be reinforced. This evaluation should be included in the statutory annual returns to the Data Protection Commissioner (paragraphs 141 & 208 and advisers report 2.2).

Governance of camera surveillance: Since the publication of the Data Protection Commissioner's *Code of Practice and Guidance on the Use of CCTV* in 2005 there have been a number of important developments in the UK in the governance and regulation of CCTV. It is apparent that some aspects of the current Jersey Code of Practice are outdated

and should be brought in line with best practice elsewhere in the UK and Europe. Our advisers have made a number of detailed suggestions (paragraph 218 and advisers report section 2.11).

It is evident that a number of CCTV operators are not compliant with all aspects of Data Protection legislation in Jersey or the Data Protection Commissioner's CCTV Code of Practice. We recommend that the Data Protection Commissioner establish processes and mechanisms to ensure compliance takes place. The creation of a CCTV register (see below) may assist in this process. CCTV operators should be reminded about the importance of compliance and the penalties arising from non-compliance. Individual CCTV operators should ensure compliance with their own CCTV Code of Practice, and thereby compliance with the Data Protection Commissioner's Code of Practice, by identifying a named employee with the responsibility for ensuring compliance and the creation of processes to monitor compliance.(advisers report section 2.12)

Specific developments and issues:

Town Centre CCTV network: The States of Jersey Police are at an advanced stage in their project to replace, upgrade and extend the current Town Centre network of CCTV cameras. This project should have involved the preparation of a detailed business case, available to the public, demonstrating the cost effectiveness of CCTV as a crime prevention measure. The Police, however, have assumed that the benefits of CCTV are well known and accepted. The Police must urgently revise their Code of Practice, improve their evaluation mechanisms which have been neglected in recent years and must provide the public with a clear statement about the functions and capabilities of their proposed new system as well as a privacy impact assessment for any proposed new locations (paragraph 34 and advisers report section 2.5).

Automatic Number Plate Recognition: The proposed new fixed ANPR system would provide the States of Jersey Police with a capability to monitor virtually all traffic movements in and out of St Helier. The system is capable of being linked to an extensive database holding significant information on Islanders. This development potentially represents a major enhancement of the surveillance powers of the Police over citizens in Jersey. It is essential

for purposes of transparency, particularly for new CCTV systems being introduced, including the States of Jersey Police ANPR system, that the principles of data connectivity are established in the *Data Protection Code of Practice and Guidance on the Use of CCTV*. The Jersey *Data Protection Code of Practice and Guidance on the Use of CCTV* should include a requirement to specify where the matching of personal data takes place, with whom and for what purposes. This is a requirement of European Data Protection law. In this respect, data should only be matched with named databases (i.e. ANPR images with the official vehicle licensing database) and not be matched with other unnamed databases. There needs to be a mechanism to regulate this (paragraphs 51-53).

Body Worn Video Cameras: The States of Jersey Police are trialing six body worn video (BWV) cameras. These cameras can protect both suspects and police officers as they are designed to provide an impartial, accurate record of incidents attended by officers. Experience elsewhere shows the introduction of these cameras has led to a sharp fall in allegations against officers. There is a robust policy in place to ensure the integrity of video evidence. A publicly available code of practice should be developed by the Police. (paragraphs 66-67).

Data matching: Data matching is a process that is relatively 'hidden' from public view. Whilst we do not want to obstruct the appropriate proportionate use of data matching it is important that the public are made aware of such processes, that they are captured by existing governance arrangements, and that safeguards are established to ensure unnecessary data matching does not take place. We recommend that any camera system that incorporates data matching as part of its purpose clearly specify this in the system's Code of Practice and on appropriate signage. This should also be specified in the Data Protection Commissioner's CCTV Register of surveillance cameras and systems. (Advisers report section 2.10 and recommendation 10)

Creating a Register of CCTV cameras: A register or census of cameras and their purposes is currently absent. Creating a register could make it easier to ensure compliance to regulations and codes of practice and place Jersey at the forefront of European best practice in this area. It would also enhance public awareness and confidence and enable political oversight. This register could be achieved through a short extension to the Data Controllers' statutory annual submission to the Data Protection Commissioner. This could comprise of a supplementary sheet, preferably one sheet of paper, capturing additional information, such

as: the number of cameras in a system, their location, the existence of a Code of Practice, primary and secondary purposes, links to other databases and perhaps some aspects of their technical capability (the latter to differentiate between different types of CCTV) **(**paragraph 80 and advisers report 2.7).

CCTV in Schools and Colleges: The primary purpose of CCTV systems in schools and colleges in Jersey is for the security of the premises and to deter intruders or petty vandalism out of school hours, although not all schools have identified a need to install cameras. CCTV cameras are not used for the purposes of monitor pupil behaviour or quality of teaching. One school, however, does use CCTV in a much more extensive way and has found CCTV to be an effective means of safeguarding pupils when they are unsupervised. In this school cameras have been installed in all classrooms. This development has been made in accordance with Data Protection advice and has not given rise to any objections from parents, students or staff (paragraphs 87).

Advanced digital capabilities: Modern digital systems, such as the system to be installed in the St Helier Town Centre, will offer the potential for advanced Video Content Analysis features, such as facial recognition, in the future. They will certainly make their introduction easy: the proposed new system could be seen as a stepping stone for more sophisticated mass surveillance. Such advances should be treated with caution. Privacy impact assessments and public consultation must take place before any such capabilities are introduced by the public sector (paragraph 100).

Privacy concerns: In general the presence of CCTV cameras in public spaces is not seen as an intrusion into privacy. However, new technologies have increased the scope and processing capabilities of camera surveillance and are often assembled in a piecemeal way without citizens being aware of their implications. Too much surveillance can fundamentally alter the relationship between the individual and the State (paragraph 116).

By the nature of the location of cameras in the Town Centre CCTV system, there is a possibility for some cameras to pan and tilt so that they can look through windows into private accommodation. We observed this possibility during our visit to the Police Control Centre. Police CCTV operators are trained to block out such views; nevertheless we believe that it is essential that property owners or tenants are made aware of the possibility of their being overlooked. The Police told us that property owners in this situation were fully aware of

the cameras as there was no attempt to hide them. It is conceivable however that as tenancy change new residents may not be alerted to the cameras. (Paragraph 20)

Codes of Practice: Every CCTV operator should have their own publicly available code of practice compliant with the Data Commissioner's Code of Practice setting out the purpose of the system, their data management procedures and security policies and their training processes for CCTV operators. This Code of Practice should be reviewed on a regular basis to ensure that the CCTV system is operating effectively against stated purposes. There is inconsistency across States departments in relation to compliance with the requirement for all CCTV operators to have their own Code of Practice – some refer simply to the Data Protection Code of Practice and Guidance in the Use of CCTV as their model whereas it should be standard practice for all public sector CCTV operators to have a specific code of practice for their operation setting out their purpose, data management procedures and security policies and information to the public on how they can contact the organisation in case of queries about their operation of CCTV (paragraphs 178 &184; Advisers report 2.11).

States of Jersey Police Force Policy: Training related to data processing and privacy principles is an essential element in the training programme for States of Jersey Police Force CCTV operators. However, the current Police Code of Practice falls short of what is seen elsewhere in the UK and Europe. The Police have acknowledged the requirement to update their policies and procedures and have assured the Panel that the documents would be reviewed as part of their project to renew and extend the current Town Centre system. Appropriate governance arrangements, an updated Code of Practice, and the introduction of auditable process must be introduced as a matter of urgency to ensure the delivery of a service in the public interest and to ensure compliance with UK and European standards and norms in the provision of CCTV. This is a necessary perquisite of the upgrade to the current Town Centre system (paragraph 193).

Retention periods: Personal data captured by CCTV is stored for varying lengths of time across different organisations using CCTV in Jersey. In almost all cases, the length of time exceeds that governing data retention in the UK and elsewhere in Europe. Given the significantly lower levels of crime and disorder in Jersey it is hard to justify why the Police and other operators require much longer periods of data retention (sometimes triple) than, say, London's Metropolitan Police, (paragraph 201).

Domestic CCTV issues: The Data Protection Office receives a significant number of enquiries relating to the potential invasion of privacy from CCTV security cameras installed in neighbouring properties with a potential overlooking into properties. Disputes over CCTV may be part of a broader conflict between neighbours. Serious cases of misuse of CCTV may constitute harassment and could be dealt with by the Police. This is a complex problem to solve, not covered currently by data protection or other legislation. One partial solution would be the introduction of planning applications for installing visually prominent cameras with a potential for overlooking. This would allow neighbours the opportunity to challenge the location of cameras. (paragraph 235 and advisers report 2.8)

We also believe that it would be helpful to neighbours if all domestic CCTV operators were obliged to register their systems with Data Protection. We acknowledge that this obligation is currently extra-statutory but we request the Data Protection Commissioner to consider and explain the implications of this suggestion. (paragraph 237)

In addition, the Data Protection Commissioner should prepare a comprehensive guidance note for those wanting to install a CCTV system at home for security purposes or to tackle anti-social behaviour (paragraph 239)

Rights of access to CCTV footage: Individuals whose images are recorded have a right to view those images and to be provided with a copy of the images. Operators' codes of practice should detail how members of the public make access requests. In practice, such requests by individuals are not common and this right is not widely known. Individuals face obstacles as it may be necessary to block out images of third parties and may be required to provide heavy justification for their request (paragraph 246).

CCTV in the workplace: There are legitimate uses of CCTV in the workplace; for example in monitoring till transactions in bars and supermarket or movements of stock in warehouses. We have received no evidence that CCTV is used in office environments in Jersey to monitor staff performance. Where employers make staff aware of the purposes and scope of this surveillance and make clear policies available on procedures for the security, processing and retention of images employees generally find no reason for concern about the overt use of CCTV. However, employees find that continuous monitoring, where this occurs, is overbearing. Complaints occur when employers use CCTV for monitoring purposes outside their stated policies and procedures (paragraph 258).

6. Recommendations

Town Centre CCTV: States of Jersey Police

1. **Recommendation**: Before any extension to the current Town centre CCTV system the States of Jersey Police must:
    - provide the public with a clear statement about the functions, capabilities and purpose of their new CCTV system;
    - re-evaluate the justification for each of their current sites; and
    - publish a privacy impact assessment statement for any proposed new locations. (paragraph 35)
2. **Recommendation:** A commitment should be made by the Minister for Home Affairs and the States of Jersey Police that no development of CCTV which includes advanced Video Content Analysis features, such as facial recognition, should proceed in the future without instigating an informed public debate and seeking approval by the States. (paragraph 101)
3. **Recommendation**: The States of Jersey Police should follow the example of local authorities in the UK and provide extensive information on their website on the Town Centre CCTV system including a map indicating the location of cameras. (paragraph 128)
4. **Recommendation**: Appropriate signage should be erected in the town centre indicating that CCTV surveillance is taking place with a contact point for members of the public with queries. (paragraph 129)
5. **Recommendation:** Appropriate governance arrangements, an updated Code of Practice, and the introduction of auditable process should be introduced as a matter of urgency to ensure the delivery of a service in the public interest and to ensure compliance with UK and European standards and norms in the provision of CCTV. (paragraph 194)
6. **Recommendation:** As part of updating their code of practice and procedures on CCTV, the States of Jersey Police should review their policy on retention periods to ensure that they are in line with current best practice. (paragraph 203)
7. **Recommendation**: The States of Jersey Police should issue regular notification to any property owners where Town Centre CCTV cameras are capable of looking through windows reminding them of procedures to preserve privacy. (paragraph 21)

Automatic Number Plate Recognition: States of Jersey Police

8. **Recommendation:** Before implementing their proposal for a fixed ANPR system around St Helier, the States of Jersey Police must consult the public and publish a privacy impact statement. (paragraph 54)
9. **Recommendation**: The *Data Protection Code of Practice and Guidance on the Use of CCTV* should include a requirement to specify where the matching of personal data takes place, with whom and for what purposes. (paragraph 55)
10. **Recommendation**: In accordance with the above recommendation, the States of Jersey Police should state clearly what databases their ANPR system will access and their purpose. Connections to any new databases should not be made without providing clear justification and seeking approval from the Data Protection Commissioner. (paragraph 56)

Body worn cameras: States of Jersey Police

11. **Recommendation**: The States of Jersey Police should provide a publically available code of practice on the purpose and use of body worn video cameras, including how personal data is processed. (paragraph 68)

Regulating CCTV: Data Protection Commissioner

12. **Recommendation** The statutory annual submission by Data Controllers to the Data Protection Office should be supplemented by additional information (as specified in the report). This should be collated into a 'CCTV register' which should be publically available. (paragraph 81)
13. **Recommendation:** An annual review of the number and types of CCTV should be presented to the Minister for Home Affairs by the Data Protection Commissioner (based on the CCTV register). This would allow some political debate and oversight. (paragraph 82)
14. **Recommendation**: A review and updating of the current *Data Protection Code of Practice and Guidance on the use of CCTV* to take account of best practice elsewhere in the UK and beyond. Improvements we would point to include:

    - A requirement for operators to include signage,
    - To integrate the principle of 'surveillance by consent',

- A requirement for operators to engage in public awareness activities,
- A requirement for operators to periodically evaluate the performance of systems,
- A requirement for operators to establish a log or register of access to CCTV control rooms and footage,
- A requirement for operators to establish training in relation to appropriate levels of individual surveillance and live targeting,
- A requirement for operators to make the public aware of surveillance systems which incorporate data matching processes,
- To establish a register of cameras and systems,
- To provide more detailed guidance on the use of surveillance cameras in domestic residential settings, and
- To incorporate a definition of public space. (paragraph 218 and advisers report 2.11)

15. **Recommendation:** The *Data Protection Code of Practice and Guidance on the Use of CCTV* should specify standardised retention periods based on the operational purposes of the CCTV systems. (paragraph 202)
16. **Recommendation**: The *Data Protection Code of Practice and Guidance on the use of CCTV* should incorporate a legal requirement to comply with the principles of surveillance by consent, including a requirement for signage, consultation and public awareness mechanisms. (paragraph 216)
17. **Recommendation:** The *Code of Practice* should also contain a requirement for all CCTV operators to make the public aware of the location of cameras, the purpose of systems and any data matching that may take place. (paragraph 217)
18. **Recommendation**: Safeguards should be introduced to ensure only appropriate and necessary data matching takes place. Any camera system that incorporates data matching as part of its purpose clearly specify this in the system's Code of Practice and on appropriate signage. This should also be specified in the Data Protection Commissioner's CCTV Register of surveillance cameras and systems. (Advisers' report section 2.10 and recommendation 10)

States Departments

19. **Recommendation:** All States departments operating 'public' CCTV systems should undertake an annual review/audit, which sets out the scope of the system, its stated purpose(s) and a range of performance indicators which can be utilised to judge the effectiveness of the system. (paragraph 168)

20. **Recommendation:** We also recommend including some comparison of the crime rates in areas observed by CCTV against those without coverage in order to assist understandings of crime displacement and to provide and evidence base to inform future camera deployment decisions. This process should be followed by a review of the appropriateness of existing camera positioning. (paragraph 169)

21. **Recommendation:** All States departments using CCTV should have their own dedicated and publicly available code of practice setting out their purpose, data management procedures, security policies and training procedures as well as information to the public on how they can contact the organisation in case of queries about their operation of CCTV. (Paragraph 185)

22. **Recommendation:** All public sector CCTV operators should be required to have a log of who has had training and when. This training should include knowledge and skills associated with the processing of personal data, the requirement to collect performance related information and the actual process of undertaking surveillance. Training should explicitly cover ethical obligations, regulatory responsibilities, privacy, issues of data handling and protection, responsible subject monitoring and access requests. Training requirements should be set out in individual Code of Practice and should be reported on in annual system reviews. (paragraph 185 and advisers report 2.13).

23. **Recommendation**: The requirement that public sector CCTV operators should undertake a minimum standard of evaluation on an annual basis to ensure that their systems are effective and appropriately sited should be reinforced. This evaluation should be included in annual returns to the Data Protection Commissioner. (paragraph 209)

24. **Recommendation**: To meet appropriate security standards a log of access to each control room should be established. This log should include details such as the name of the visitor, time of visit, purpose and name an employee responsible for escorting

the visitor. Visitors should be required to present a recognised form of identification before being granted access to a surveillance camera operations centre. (Advisers' report section 2.4)

25. **Recommendation:** All requests to view footage are recorded in a log, not just those incidences where footage is legally obtained for investigations. This log should apply to anyone not working, at that time, in the CCTV control room. The log should include details of the name of the person requesting footage, reason, time of request, and name of the person granting the request. (Advisers' report section 2.4)

26. **Recommendation:** We recommend that image retention periods are limited to a maximum 31 days across public surveillance camera operations. This is common practice elsewhere in the UK and the EU. This maximum data retention period should be specified in the Data protection Commissioner's CCTV Code of Practice. (advisers' report)

Domestic CCTV issues

27. **Recommendation**: The Panel recommends that the Planning Minister gives serious consideration to reviewing the classification of CCTV as permitted development and follows the example of Scottish legislation on this matter. (paragraph 236)
28. **Recommendation**: The Data Protection Commissioner should prepare a comprehensive guidance note for those wanting to install a CCTV system at home for security purposes or to tackle anti-social behaviour. (paragraph 240)

7 Introduction

1. CCTV surveillance cameras are deployed extensively throughout the UK and in Jersey. We are used to seeing them monitoring movements in all public areas, in streets, banks, shops, airports, bus stations. They are unremarkable. Used appropriately they can be a valuable tool contributing to public safety and security and in protecting people and property.

2. However, there is also an increased risk of interference with a citizen's right to privacy. The UK first Surveillance Camera Commissioner recently warned: '*CCTV systems capable of* identifying *and tracking a person's face from half a mile away are turning Britain into a Big Brother society. New high-definition cameras are being rolled out across UK cities without public consultation into the intrusion they pose'*, Andrew Rennison told the Independent. '*The increasing sophistication of surveillance technology is becoming so serious that Britain may be in breach of its own human rights laws*,' he said.

3. The Scrutiny Panel believes that the public in Jersey deserves to have confidence that the use of camera surveillance is in the 'public interest'. This is especially the case for the Town Centre CCTV system operated by the States of Jersey Police. Public support for CCTV can be enhanced through the introduction of improved governance arrangements, including the introduction of a publicly available Code of Practice for the Town Centre CCTV system, performance audit and public engagement. The overall aim of the recommendations in this Scrutiny review then is to promote public awareness and debate about the capabilities of the various systems in use in the Island.

4. In the first part of this report we look at the scale of usage of CCTV by the States of Jersey and by commercial and non-commercial agencies. In the next section of the report we look at public attitudes to CCTV. In general, CCTV is seen as benign, an anti-crime measure which brings few disadvantages of which people are conscious. The presence of CCTV cameras in public spaces is not seen as an intrusion into privacy, a concept associated with the home. However, as new technologies develop the capabilities of camera surveillance we believe that, for the public to retain this confidence in the appropriate use of CCTV surveillance, it is essential that CCTV operators engage

with the public in an open and transparent way to explain the capabilities and limitations of their systems.

5. There is considerable debate across Europe about how the effectiveness of CCTV cameras might be measured. In part three of our report we have looked at some of the research in this area and taken account of the views of those who believe that the expectations for CCTV are unrealistic. Reviewers in the UK have noted that CCTV is the single most heavily funded crime prevention measure operating outside the criminal justice system, accounting for more than three quarters of the total spending on crime prevention by the British Home Office. Here in Jersey we have found that methods of demonstrating the effectiveness of cameras installed by both the States of Jersey Police and other States departments have been neglected. We believe that a regular analysis and evaluation of the efficacy of States CCTV systems must be provided to the public.

6. In part four of our report we look at the governance of CCTV in Jersey and in particular at the Data Protection Code of Practice and Guidance on the Use of CCTV (2005). CCTV creates data in the form of images which can be stored and retained for extended periods of time for subsequent review and can be used to identify individuals for a variety of purposes. The protection of privacy and rules for the appropriate processing of data and the basis for Data Protection legislation and for these reasons Data Protection is the relevant body to regulate CCTV. We make a number of recommendations in this report for the Data Protection Commissioner. In doing so we acknowledge the independence and autonomy of the Office of Data Protection. However, we believe that it is important that the regulation of CCTV, as with other data protection issues, is kept up to date with recent developments.

7. The Code of Practice applies principally to the public sector and there are limited controls over commercial systems although the Code sets out guidance for the following of good practice. The UK has recently seen the establishment of a Camera Surveillance Commissioner and the publication by the Home Office of a Surveillance Camera Code of Practice (June 2013). The concept of ‘surveillance by consent’ is fundamental to this new Code and we believe that the local Jersey Code of Practice needs to be updated in a number of ways to keep up to date with developments in the UK. This task will undoubtedly have resource implications for the Data protection office which is already

dealing with the implications of the introduction of Freedom of Information legislation in Jersey.

8. Finally, an increasingly common problem with CCTV was drawn to our attention, namely the potential intrusion into privacy by the installation of cameras on neighbouring residential properties. There is no simple solution to this issue as existing legislation does not cover this issue. We looked for a legal remedy which we believe could be provided through an amendment to the planning development controls. This would provide homeowners with the opportunity to challenge the validity of cameras which clearly have the potential for overlooking without compromising the cameras effectiveness for security purposes.

8 The Prevalence of Camera Surveillance

The scale of usage of camera surveillance in Jersey by the States of Jersey, commercial and non-commercial agencies.

Public Sector CCTV: survey

9 The Panel carried out a survey of the use of CCTV systems all States departments. This showed that the States currently operate more than 1,300 CCTV cameras and 10 Automatic Number Plate Recognition (ANPR) cameras. (see appendix for detailed results)

10 The principal purposes given for operating CCTV systems range from:

- the prevention, investigation and detection of crime;
- the gathering of evidence and the prosecution of offenders;
- monitoring the security of premises and deterring intruders;
- discouraging vandalism and antisocial behaviour;
- the protection of staff from aggression or malicious allegations;
- searching for missing or vulnerable persons;
- the improvement of customer services;
- personnel and employee administration.

11 Some departments have specific requirements, for example:

- the States of Jersey Police (SOJP) and the Jersey Customs and Immigration Service (JCIS) monitor detainees held in custody cells at Police Headquarters (15 cameras) and the harbour (15 cameras);
- HM Prison La Moye operates 245 cameras for the protection and security of staff and prisoners;
- The ports of Jersey require CCTV to meet national security regulations at the ports of Jersey;
- Transport and Technical Services have 187 cameras monitoring vehicle movements and congestion in car parks;
- CCTV is fitted as a standard safety feature standard on all modern fire engines.

Town Centre CCTV: current system

12 While the majority of cameras operated by the States of Jersey are focused on the interior and immediate surroundings of buildings for security purposes, the States of Jersey Police operate a network of 23 cameras in the open public space in the town centre. The stated purposes of this system are:

- The reduction, prevention and detection of crime and criminal activity
- Evidence gathering
- Policing displays such as Liberation Day, Battle of Flowers
- Searching for missing/vulnerable people

13 The cameras are located at strategic points and monitor activity in a range of streets throughout St Helier, focussing predominantly on 'hot spots' in the night time economy where large numbers of people tend to congregate outside clubs and bars at the weekends.

14 The States of Jersey Police also have access to other public space cameras: they operate joint systems with the Jersey Customs and Immigration Service at the Airport (21 cameras) and St Helier Harbour (6 cameras) and can access systems in the public parks (Millennium 10 and Howard Davis 6) as well as private systems at locations such as Les Quennevais precinct and Bonne Nuit harbour.

15 The first town centre system for St Helier, comprising 12 cameras, was implemented in 1995/6 with further cameras added at various points in time, for example with the development of the Waterfront.

16 In Jersey the States of Jersey Police took the initiative to establish town centre surveillance cameras in the absence of any clearly defined alternative body. As a consequence, and unusually, the Police have lead responsibility for the Town Centre Network – in the UK town centre systems are operated by the local authority, although police forces often have joint control rooms.

17 In the UK broader functions, such as traffic management and parking control, are often included with Town Centre CCTV network. The latter has been controversial in the UK where councils have been accused of raising revenue through spying on motorists.[1] In Jersey the cameras in the town centre are not used to manage the flow of traffic nor to deal with illegal parking.

18 The cameras in the town centre are operated on a continual basis with live feeds to monitors in a room situated next to the Force control Room at Police Headquarters. The screens are only actively monitored by civilian support officers in the Force Control Room at busy periods. The Honorary Police assist the States of Jersey Police at weekends. Officers in the Force Control Room can access the cameras easily at any point in response to particular events.

19 For the most part the focus of the cameras is pulled back to give a broad, general view of the streets; however, operators can pan, tilt and zoom (x30) the cameras in order to pick up particular incidents and track individuals.

20 **Key Finding**: By the nature of the location of cameras in the Town Centre CCTV system, there is a possibility for some cameras to pan and tilt so that they can look through windows into private accommodation. We observed this possibility during our visit to the Police Control Centre. Police CCTV operators are trained to block out such views; nevertheless we believe that it is essential that property owners or tenants are made aware of the possibility of their being overlooked. The Police told us that property owners in this situation were fully aware of the cameras as there was no attempt to hide them. It is conceivable however that as tenancy change new residents may not be alerted to the cameras.

21 **Recommendation:** The States of Jersey Police should issue regular notification to any property owners where Town Centre CCTV cameras are capable of looking through windows reminding them of procedures to preserve privacy.

[1] http://www.bbc.co.uk/news/uk-politics-24291467

Town Centre CCTV upgrade

22 The States of Jersey Police are currently in the process of renewing and upgrading the Town Centre system which has been in place since 1995 and is operating with outdated components which are now of poor quality and are difficult to replace. The project will include the replacement of the current analogue system for digital cameras and recording.

23 The CCTV upgrade project has been ongoing since 2010; however, delays to the planned new Police Headquarters has affected the CCTV upgrade project as it was originally planned not to replace the Town centre system until the new headquarters was operational. However it has now been agreed to start replacing the system from the end of 2013. The project will be carried out in phases due to the complexity of the project. The first stage (end 2013) will be to replace the recording system. Stage two (Q2 2014) will see the replacement of the town centre cameras, like for like. The zoom capability of the new cameras will be on a similar level to the current system (x30). Mega pixel capabilities would require high storage facilities and would be beyond the current budget. There is no capacity for retrospective zoom. There is no plan to introduce analytics (eg tracking or facial recognition) at this stage – the system however will be capable of adding analytic features in the future (see further discussion on analytics below).

24 The new cameras will not be linked to the proposed new ANPR system (see further discussion on ANPR below).

25 The Police are currently looking at the possibility of wireless transmission of images back to Police Headquarters which will reduce ongoing revenue costs. There is a downside to wireless transmission which might be less reliable than the current fibre cable system.

26 The Police have also identified an operational desire to increase CCTV coverage in the town area with the possible addition of six cameras in areas identified as potential hot spots not covered by existing cameras. This development will take account of the changing topography of the St Helier night time economy, for example the location of new night clubs while others have disappeared. Cheapside, Snow Hill and St Aubin Harbour area are other potential sites; however, no firm decisions or sites have yet been identified. This element of the project is subject to confirmation of further funding and

public consultation on the proposed new locations. Funding for an extension to Castle Quays, however, has already been agreed under a planning obligation.

27 We were informed that, to date, the project has focussed on the technical elements of the new system. Ongoing project planning will include, in due course, an impact analysis, based on incident analysis, victim survey information and consultation with key stakeholders such as proprietors of bars and clubs.

28 The CCTV upgrade project has been linked with similar upgrades to replace existing cameras and install additional cameras for States of Jersey Police systems at the Airport (25 cameras) and St Helier Harbour (28 cameras).

29 In the early stages of the project it was anticipated that a £40,000 CSR saving could be achieved; however, this has now been revised and no significant savings will be achieved. Instead the project has been designated a capital project.

30 An application was made to the Criminal Offences Confiscation Fund (COCF) to fund all three systems. The following funding was requested:

- Town Centre £400,000
- Airport £100,000
- Harbour £80,000
- 10% contingency £58,000

31 An additional sum of £25,000 was found from savings on a previous project. This was used for the custody suite and renewal of the Police Headquarters estate requirements.

32 We asked the Acting Chief Inspector to describe how the States of Jersey Police intended to engage with the public on the forthcoming extension of the town CCTV network. He replied that appropriate public consultation would be planned once the technical elements of the project had been finalised and he promised to keep us informed.

33 Our advisers commented: ‘Further clarification is required concerning the evidence used to inform decisions over camera deployment and network expansion. Evidence collected thus far points to a high value placed on tacit and experiential judgment. These are

appropriate forms of information although one would expect such information to be supplemented by more objective measures such as offence mapping and public engagement.'

34 **Key Finding**: The States of Jersey Police are at an advanced stage in their project to replace, upgrade and extend the current Town Centre network of CCTV cameras. This project should have involved the preparation of a detailed business case demonstrating the cost effectiveness of CCTV as a crime prevention measure. The Police however have assumed that the benefits of CCTV are well known and accepted. The Police must urgently revise their code of practice, improve their evaluation mechanisms which have been neglected in recent years and must provide the public with a clear statement about the functions and capabilities of their proposed new system as well as a privacy impact assessment for any proposed new locations.

35 **Recommendation**: Before any extension to the current system the States of Jersey Police must

- provide the public with a clear statement about the functions, capabilities and purpose of their new CCTV system;
- re-evaluate the justification for each of their current sites; and
- publish an privacy impact assessment statement for any proposed new locations.

Other States of Jersey Police developments

Automatic Number Plate Recognition

36 The States of Jersey Police currently use a mobile Automatic Number Plate recognition (ANPR) camera fitted to an unmarked van to alert for vehicles of interest, such as those driven by suspected disqualified drivers. The system works best when the vehicle with the ANPR reader is stationary and the cameras are set to record vehicles which pass it by. Once an alert is read the ANPR operator then radios another police unit(s) further down the road to stop the vehicle. The Roads Policing Unit commented that the system can be resource intensive and in recent times other commitments had taken preference over this system.

37 The intelligence databases employed by the ANPR system are managed by the Force Intelligence Bureau. They receive intelligence which can then be loaded on the database in respect of uninsured drivers, wanted individuals (for example, arrest orders from the court and disqualified drivers) and stolen vehicles (albeit few in number in Jersey).

38 The current system has not been used effectively and its recent use has been restricted. The Roads Policing Unit commented: '*We tended to have too much information on the system which meant that we were getting a lot of "hits" which did not result in any prosecutions/ arrests. Should the ANPR be re-introduced under a different format consideration should be given to drastically reducing the number of vehicles on it and maintaining the accuracy of the system.'*

39 The Police are reviewing this facility with a view to establishing a static network predominantly based around St Helier with links to systems operating at the ports and being developed for car parks (see further discussion below).

40 The Jersey Customs and Immigration Service also use ANPR to record all vehicle movements in and out of the Island. Transport and Technical Services are currently trialling the use of ANPR for a new vehicle parking charge system.

41 The States of Jersey Police are examining a proposal to replace their current mobile ANPR facility with a static ANPR system situated on the main roads entering St Helier which would be capable then of monitoring virtually all vehicle movements through the town. The project is at an early stage: there are no firm plans for this but funding has been identified through the Criminal Offences Confiscation Fund (COCF).

42 As previously noted, the system has significant resource implications for the States of Jersey Police if it is to be used more effectively than the current system. The Police Officer responsible for the project commented: *We need the ability to deal or at least to consider dealing with whatever may be 'pinging' at that time, hence the requirement for a real tight set of databases operating at any one time i.e. intelligence led, aligned to priorities at that time etc.*

43 The fixed system would have a direct feed into the Police Force Control Room. It would be linked to the ANPR systems operated at Elizabeth Harbour by the Customs and

Immigration Service and may be linked to the car parks operated by Transport and Technical Services (subject to approval of this system following the current trial).

44 This form of ANPR system has proved controversial in the UK. The installation of seven ANPR cameras around the town of Royston by the Hertfordshire Constabulary was dubbed a 'Ring of Steel' and criticised by privacy campaigners for infringing car drivers' rights.

45 The UK Information Commissioner found that the Royston scheme was 'unlawful', breaching the first principle of the Data Protection Act (processing personal data fairly and lawfully) and 'excessive', breaching the third principle of the Act (relating to the amount of data collected; personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed').

46 Hertfordshire Constabulary were issued with an enforcement notice ordering the force to stop processing people's information in this way, unless they could justify the ANPR cameras use by way of a proper privacy impact assessment, or similar such assessment.[2]

47 In response, Hertfordshire Constabulary said that the enforcement notice was unnecessary. They would continue to use the system which had been effective in cutting crime but would ensure that they gave an adequate explanation as to why it was necessary.[3]

48 The concerns about ANPR relate to the use of data matching. The UK campaign group Liberty expressed concern that the use of ANPR has expanded enormously without any real public debate or knowledge: *'This technology, originally used to monitor* unregistered *vehicles, is now routinely being used by the police to locate vehicles (and their owners) that might appear on other – and often dubious – police databases. There is almost no binding regulation about how this technology is to be used, who can be targeted using it,*

[2] http://www.ico.org.uk/news/latest_news/2013/police-use-of-ring-of-steel-is-disproportionate-and-must-be-reviewed-24072013
[3] http://www.newlistener.co.uk/home/royston-anpr-array-unlawful/

how long images are to be stored for and for what purpose. A database of this magnitude raises real privacy concerns and requires strong regulation.'[4]

49 Our advisers commented: 'This issue has received increasing attention in European data protection legislation. Clarification is required concerning the matching of CCTV images to data held on formerly distinct databases and what happens to new information that is crated from the merger of these different information systems. This is not covered by existing Codes of Practice.'[5]

50 Charles Farrier, of NO-CCTV, provided the Panel with a recently published report entitled 'What's wrong with ANPR'. In this paper he suggests ways in which ANPR might be used without the need to include mass surveillance capabilities. He maintains that it is possible to use the ANPR cameras for the stated aims, namely enforcement of motoring issues such as unpaid tax or insurance as well as stopping vehicles of known wanted criminals without tracking the movements of law abiding citizens. It is not necessary for the system to store any data.

51 **Key Finding:** A new fixed ANPR system potentially provides the States of Jersey Police with a capability to monitor virtually all traffic movements in and out of St Helier. The system which could be joined up to ANPR systems at Elizabeth Harbour and car parks can potentially be linked to an extensive database holding significant information on Islanders.

52 **Key Finding**: It is essential for purposes of transparency, particularly for new CCTV systems being introduced, including the States of Jersey Police ANPR system, that the principles of data connectivity are established in the *Data Protection Code of Practice and Guidance on the Use of CCTV*.

53 **Key Finding**: The Jersey *Data Protection Code of Practice and Guidance on the Use of CCTV* should include a requirement to specify where the matching of personal data takes place, with whom and for what purposes. This is a requirement of European Data

[4] https://www.liberty-human-rights.org.uk/human-rights/privacy/cctv-and-anpr/index.php accessed 11.10.13
[5] Initial thoughts on visits

Protection law. In this respect, data should only be matched with named databases (i.e. ANPR images with the official vehicle licensing database) and not be matched with other unnamed databases. There needs to be a mechanism to regulate this.

54 **Recommendation:** Before implementing their proposal for a fixed ANPR system around St Helier, the States of Jersey Police should consult the public and publish a privacy impact statement.

55 **Recommendation**: The *Data Protection Code of Practice and Guidance on the Use of CCTV* should include a requirement to specify where the matching of personal data takes place, with whom and for what purposes.

56 **Recommendation**: In accordance with the above recommendation, the States of Jersey Police should state clearly what databases their ANPR system will access; connections to any new databases should not be made without providing clear justification and seeking approval from the Data Protection Commissioner.

Body Worn Video Cameras

57 The States of Jersey Police have recently been trialling six body worn video (BWV) cameras. Forty police forces in the UK are already using these devices. As a result of the success of this trial, the Police are now considering extending the use of cameras to all officers on the beat, currently numbering about thirty. This announcement was made as the report was being finalised[6] so it has not been possible to include an examination of the report on this trial; however, this report will be studied by the Panel.

58 The BWV cameras are designed to enhance opportunities for evidence capture, providing an impartial, accurate record of incidents attended by officers. They may help to secure a successful prosecution in cases where otherwise the police officer word was the only evidence.[7]

[6] All Police to wear uniform cameras? Jersey Evening Post, dated 5 December 2013
[7] http://www.newscientist.com/article/mg22029404.400-bodyworn-cameras-put-police-evidence-beyond-doubt.html#.Umg9tvm-2uI

59 BWV cameras are an overt method of gathering evidence. Wherever possible the officer will inform the subject that they are being recorded by CCTV. Officers are trained to avoid 'collateral intrusion', that is the unnecessary recording of third parties.

60 The Police expect that this system will be particularly useful in domestic violence incidents where the victim is often reluctant subsequently to pursue a complaint. They will also contribute to a decrease in assaults on officers and raise professional standards among police officers. The Police officers are under increased scrutiny through the use of the cameras.

61 The BWV cameras are not in operation continuously: the police officer must trigger the recording mechanism when they recognise that an incident or an appropriate interview with a subject is taking place. Data from BWV cameras can be downloaded at the police station and relevant incidents tagged for further investigation either by the officer or the reactive investigation team. There is an automatic electronic audit trail for the use of the images.

62 Recordings do not replace the need for formal written statements from victims or witnesses but can be used as supporting evidence for the statements.

63 Civil liberty groups have given qualified support to BWV cameras because of their potential to serve as a check against the abuse of police power. However, there are provisos: the recordings of interactions with suspects must be complete, that is they must not be edited 'on the fly' so that they only record what backs the police version of events; secondly, the back-office data storage system for video evidence must be secure, accessible to lawyers and defendants.[8]

64 We were provided in confidence with a copy of the States of Jersey Police Force Policy on Body Worn Video. This provides detailed guidance to officers using the devices. In summary:

- The officer should record as much of an incident as possible

[8] Ibid

- The recording must be incident specific
- The user should make a verbal announcement to indicate why the recording has been activated, including date, time and location
- Persons present should be informed
- Recording must continue uninterrupted
- A verbal announcement should be made to indicate the end of the recording, including the reason for ending

65 In general, the BWV user should record entire encounters from beginning to end without interrupting the recording. There may, however, be incidents where it might be necessary for the user to consider stopping the recording and examples are given in the guidance, such as sensitivity connected to faith, where filming in domestic circumstances could be an issue. The reasons for interrupting or ceasing to record an ongoing incident must be recorded in the officer's police notebook. The policy is clear that under no circumstances must any images be deleted; such action may result in disciplinary proceedings.

66 **Key Findings**: The States of Jersey Police are trialing six body worn video (BWV) cameras. These cameras can protect both suspects and police officers as they are designed to provide an impartial, accurate record of incidents attended by officers. Experience elsewhere shows the introduction of these cameras has led to a sharp fall in complaints against officers.

67 There is a robust policy in place to ensure the integrity of video evidence, which has been made available to the Panel. In line with our other recommendations, we believe that the States of Jersey Police should provide a publically available code of practice on the purpose and use of these cameras, including how personal data is processed.

68 **Recommendation:** the States of Jersey Police should provide a publically available code of practice on the purpose and use of body worn video cameras, including how personal data is processed.

CCTV in the Private sector

69 There are many more CCTV camera surveillance systems in the private sector operating in areas to which the public have access: supermarkets, the bus station, cinema, petrol

stations, banks, pubs, hotels, tourist attractions, community centres, schools and restaurants offices all make use of camera surveillance.

70 We spoke to one of the four principal security companies installing CCTV systems who reported increasing interest in systems in the Island. A number of general electrical companies also sell systems but with limited back up. It is also possible to buy relatively cheap systems from the shelf at DIY stores or from the internet.

71 Retail stores use CCTV as a method of reducing the impact of theft on their business. In Jersey most CCTV in stores is not continually watched over and so many thefts are not instantly detected. If however an item is found to be missing, it is then possible to review footage and see if the offence has been caught on camera.

72 The Chamber of Commerce, Retail and Supply Committee, said that CCTV had been introduced into retail stores by many of its members in response to increasing instances of theft. They told us that retailers needed to use as many ways as possible to reduce the impact of theft on their business, the main defence being staff on the sales floor but CCTV was an important backup for them together with other methods, mainly security tagging systems and loss protection detectives[9].

73 A major supermarket chain told us that all their till transactions are monitored by CCTV. Till loses have been reduced when cameras are placed above till points. Tills covered by CCTV also assist in any potential customer fraud situation such as stolen cheques.

74 CCTV also helps to protect staff. There is a potential for violent or abusive behaviour to situations, such as the withholding of a credit card if asked to do so by the credit card company after a decline.

75 The Panel visited a major St Helier hotel which operates 156 cameras monitoring virtually all public space within the hotel, bar and its night club. The manager told the Panel that cameras are regarded by customers and staff as an expectation for the security of the hotel. We were told that CCTV had been effective in monitoring staff

[9] Chamber of Commerce written submission,

transactions at the bar reducing till losses from staff fraudulently serving customers with extra drinks to virtually nil.

76 CCTV cameras are increasingly commonplace on all forms of public transport. Liberty buses are fitted as standard with between 6 to 8 cameras, both inside and outside the vehicles. They monitor the safety of passengers, particularly accessing and leaving the buses; mitigate complaints or claims from customers and provide evidence in case of road accidents. A number of taxis drivers are now fitting their vehicles with cameras in order to enhance security for the drivers.

77 It is very difficult to gauge accurately the extent of CCTV coverage in the private commercial sector in Jersey. Where images are recorded any business using CCTV camera surveillance is required to register their systems with the Data Protection Commissioner; however, the Commissioner told the Panel that she was sure that there are many more systems operating in the Island than are notified to her office[10].

78 Some businesses remain unaware of their obligations regarding CCTV. Efforts are made by the Data Protection Office to inform businesses of the obligation to register their systems, particularly when omissions come to light; however, resources generally preclude proactive investigations into the policies and practices of most companies.

79 The States of Jersey Police has compiled its own register of premises with CCTV availability. Whenever a crime occurs the police will investigate the location of CCTV in the vicinity to establish whether there might be relevant or recoverable CCTV footage. The list, however, is for the guidance of officers only and is not definitive.

80 **Key Finding**: A register or census of cameras and their purposes is currently absent. Creating a register could make it easier to ensure compliance to regulations and codes of practice and place Jersey at the forefront of European best practice in this area. It would also enhance public awareness and confidence and enable political oversight. This register could be achieved through a short extension to the Data Controllers' statutory annual submission to the Data Protection Commissioner. This could comprise

[10] Public hearing, 26.06.13, page 22

of a supplementary sheet, preferably one sheet of paper, capturing additional information, such as: the number of cameras in a system, their location, the existence of a Code of Practice, primary and secondary purposes, links to other databases and perhaps some aspects of their technical capability (the latter to differentiate between different types of CCTV).

81 **Recommendation** The statutory annual submission by Data Controllers to the Data Protection Office should be supplemented by additional information (as specified above). This should be collated into a 'CCTV register' which should be publically available.

82 **Recommendation:** An annual review of the number and types of CCTV should be presented to the Chief Minister for Home Affairs by the Data Protection Commissioner (based on the CCTV register). This would allow some political debate and oversight.

CCTV in Schools and Colleges

83 Many schools and colleges operate CCTV systems for the security of the premises and to deter intruders or petty vandalism out of school hours. Not all schools, however, particularly those in the more rural areas of the Island, felt the need for this form of security.

84 Active monitoring does not take place: CCTV is not used to monitor entry to school premises during school hours nor to monitor pupil behaviour.

85 One private school, however, uses CCTV to ensure effective safeguarding and counter-bullying measures and has recently completed installation of cameras in all classrooms as well as in corridors and public spaces. No cameras were installed in areas where there was a reasonable expectation of privacy, such as changing rooms. CCTV was not used to monitor teaching in school.

86 The Panel invited the head teacher to discuss how the decisions had been taken to extend camera use in this way. He told us that the CCTV system had been introduced originally in response to requests from parents for the school to take effective action to deter illegal drug use on part of its external grounds (whilst the school was not in

session), also to combat a spate of vandalism to its buildings & vehicles which had occurred at night and at the weekend. Once installed the extended use of CCTV as a means of investigating cases of bullying where it was often a case of one student's word against another had seemed to be a logical step. CCTV was only used when necessary as back up to normal staff monitoring and person to person discussion with pupils. Following advice from the Data Protection Commissioner's office this use had been declared as part of the school's policy on the use of CCTV. No reservations had been raised by staff, parents or students regarding the extent of potential surveillance.

87 **Key Finding**: The primary purpose of CCTV systems is for the security of the premises and to deter intruders or petty vandalism out of school hours, although not all schools have identified a need to install cameras. CCTV cameras are not used to monitor pupil behaviour. One school, however, does use CCTV in a much more extensive way and has found CCTV to be an effective means of safeguarding pupils when they are unsupervised. In this school cameras have been in installed in all classrooms. This is in accordance with Data Protection principles and has not given rise to any objections from parents, students or staff.

Technological advances: public sector

Current capabilities

88 It is beyond the scope of the Scrutiny review to examine in detail the technical quality of CCTV systems and their images across States departments. This varies according to the priorities of each department. Almost all systems share fundamental capabilities: an ability to operate continuously, monitoring and recording activity within a given field as well as providing a live feed to screens within a control room and record activity within a given field. For the most part cameras are not actively monitored unless there are indications of specific interest in locations or individuals.

89 Many cameras are positioned in order to give maximum operational coverage without quality recognition of individuals. Some cameras may be remotely operated and directed on to particular individuals or incidents through pan, tilt and zoom facilities in response to intelligence information. Individual recognition may be achieved within a certain distance (eg 50 to 100m) but will be reduced during hours of darkness.

90 Data can be retained, depending on storage capacity, for periods of some months but will usually be overwritten or deleted automatically after a defined period (typically 30 days although we were told that many systems in Jersey retain images for much longer). Data can be retrieved from the recorded storage for evidential purposes and saved to video or disc.

91 A number of States systems, including the Town Centre network and SOJP and JCIS systems at the Airport and Harbours are operating with outdated systems. The SOJP reported that the technology and components of the current analogue system, viewed by us, were soon to be obsolete, making servicing and repair difficult and costly. We also observed JCIS systems where the quality of images was poor and the technology used to review the CCTV footage was cumbersome and inefficient.

92 Modern high definition, digital CCTV systems provide an efficient management module and high resolution images. Furthermore, they have many computer controlled technologies that allow them to identify, track, and categorize objects or persons in their field of view.

Advanced Video Content Analysis

93 Through Video Content Analysis (VCA) systems can detect unusual patterns of behaviour in the environment or anomalies in a crowd of people such as for instance a person moving in the opposite direction in airports where passengers are only supposed to walk in one direction out of a plane. VCA also has the ability to track people on a map by calculating their position from the images. It is then possible to link many cameras and track a person through an entire building or area. This can allow a person to be followed without having to analyse many hours of film.

94 Facial recognition facilities are being developed which will allow individuals to be automatically identified from a facial database. This type of system has been proposed to compare faces at airports and seaports with those of suspected terrorists or other undesirable entrants. This form of mass surveillance has been ineffective to date because of the low discriminating power of facial recognition technology and the very

high number of false positives generated. Nevertheless, future developments will continue to improve the capabilities of CCTV surveillance.

95 No States department in our survey reported any intention to introduce analytic features into their systems.

96 A major CCTV installer informed us that there was little interest from the commercial sector in Jersey at present in high definition systems with advanced analytical features. However, the position might change in the future as such systems became more economical.

97 The States of Jersey Police informed us that these forms of advance analytics are not being considered at present for the new Town Centre and Harbours and Airport systems. Such features are not regarded as operational requirements given the relatively low level of crime and public disorder in Jersey. Furthermore the costs of including such features within the design of the new systems would be substantial.

98 We were informed that the new digital CCTV system for St Helier would essentially be a replacement for the existing analogue, fibre cable system. The zoom power would be similar to the current system (x30); mega pixel capabilities required high storage facilities and would be beyond the current budget. A wireless solution was under consideration as this could have financial savings over fixed fibre cables but there were risks of hacking or blocking and reduced reliability.

99 However, it should be noted that new modern digital systems will make it easy to introduce advanced analytics in the future, whereas current analogue systems make this very difficult. The significance of the new system should not be underestimated or downplayed

100 **Key finding:** Modern digital systems, such as the system to be installed in the St Helier Town Centre, will offer the potential for advanced Video Content Analysis features, such as facial recognition, in the future. They will certainly make their introduction easy: the proposed new system could be seen as a stepping stone for more sophisticated mass surveillance. Such advances should be treated with caution. Privacy impact

assessments and public consultation must take place before any such capabilities are introduced by the public sector.

101 **Recommendation:** A commitment should be made by the Minister for Home Affairs and the States of Jersey Police that no development of CCTV which provides in the future for advanced Video Content Analysis features, such as facial recognition, should proceed without instigating an informed public debate and seeking approval by the States.

9 Public attitudes towards camera surveillance

Online public survey

102 We conducted an online public opinion survey on the Scrutiny website to explore public awareness and attitudes towards camera surveillance in Jersey. 46 responses were received between 25 June and 9 September 2013. A summary of the results of the survey are shown in Appendix Two of this report. A full report from the survey can be accessed on the scrutiny website.

103 The limitations of this survey should be noted:

- It is clearly only a very small sample of public opinion.
- Respondents were self-selecting – there was no attempt to ensure a scientifically balanced representation of the population as a whole.
- The survey did not test whether the respondents understanding of the technological capabilities of the CCTV systems or how they are used.

104 It is not possible therefore to draw specific conclusions from this survey with any confidence; however, some general observations can be made.

105 The response to our survey showed general public support for CCTV and revealed no strong evidence of concern among respondents about CCTV in public spaces:

- 65% disagreed with the statement that CCTV surveillance in public areas in our Island today was excessive;
- 59% disagreed with the statement that public expenditure on CCTV cameras should be reduced;
- 47 % however said that they did not want to see any additional CCTV

106 A commonly held view was reflected in one comment: '*If you have nothing to hide you have* nothing *to fear from better security in both public and private places. I do not mind how many CCTV cameras are used as I feel they are there for my protection and security, not to spy on me or to intervene in my freedom of movement.'*

107 There was more ambivalence about the potential intrusion of CCTV near homes and in the work place: 47% of respondents agreed that CCTV near their homes infringed their personal rights to privacy and 55% agreed that the presence of CCTV in the workplace infringed their personal right to privacy. There was a strong feeling that information on surveillance and access to data collected were important (79% and 93% respectively).

108 A fully scientific survey into public attitudes to the deployment of CCTV in public spaces was carried out in 2004 by the Information Commissioner's Office (ICO). The ICO found that CCTV in public places is not generally considered to intrude on personal privacy. '*This may be because individuals expect to be seen when out and about in public places, and they behave and dress accordingly. They are already 'on show', as it were. Being watched by a camera does not appear very different from being looked at by passers-by*.'[11]

109 **Key Finding**: Public sector CCTV is generally perceived as benign, an anti-crime measure which brings few disadvantages of which people are conscious. CCTV in public spaces is not thought to intrude on personal privacy, a concept associated with the home. However, there is no real evidence that the public have a good understanding of the technological capabilities of CCTV systems or how they are used.

Concerns relating to the extent and purpose of intrusion into people's lives

110 On the other hand, a number of people hold the view that the extent of mass surveillance by the state, of which CCTV is just one overt element, should be a cause for concern.

111 Mr. M. Dun, whose topic proposal initiated our review, called for greater political oversight of CCTV operations and identified the following key issues:

- The risks of discrimination in targeting types of individuals for observation;

[11] Public attitudes to the deployment of surveillance techniques in public places, ICO March 2004

- A requirement for operators to be trained in data protection and privacy issues;
- The capability of cameras to record conversations as well as images;
- The lack of public awareness and appropriate signage.12

112 Civil liberty groups argue that data protection legislation has failed to keep up with technological changes and as a result there is a risk that unregulated CCTV may pose a threat to our way of life. The UK campaigning group Liberty comment: '*We are unlikely to wake up one morning with the feeling that we are suddenly under much more surveillance than the day before. This is because surveillance apparatus is assembled in a piecemeal way and often under the radar. Too much surveillance can fundamentally alter the relationship between the individual and the State and the experience of widespread visual surveillance may well have a chilling effect on free speech and activity*.[13]

113 Charles Farrier, co-founder of No-CCTV, in his submission for our review commented on the implications of mass surveillance by the State: *The oft repeated but little understood catchphrase "nothing to hide, nothing to fear", consistently used to justify video surveillance, turns the usual law enforcement requirement of "reasonable* suspicion*" upon its head. In the case of surveillance cameras information is recorded regardless of the existence of specific cause. Cameras record continuously, as opposed to recording only selective incidents related to law enforcement activities, and so information on thousands of innocent people engaged in activities irrelevant to the supposed justification for the cameras is collected. …… The State is a particular special case for us because the State has the power to deprive people of liberty, has legitimate use of force and other things like that.*[14]

114 The Data Protection Commissioner identified where she believed that CCTV might pose a threat to privacy. She said that for the individual the impact of CCTV surveillance in public spaces was minimal, if any at all: images are not processed; they just sit there

[12] Preliminary discussion with the Panel, 02.05.13
[13] https://www.liberty-human-rights.org.uk/human-rights/privacy/cctv-and-anpr/index.php accessed 11.10.13
[14] Ibid

and nothing happens. If there is no incident, if nothing else is triggered, the images get deleted after a period of time. However, she went on to say: *it is the implications of the processing in terms of privacy, which is terribly important... if every time your face hit a camera something else was triggered*.[15]

115 An example of the potential impact of CCTV surveillance on the privacy of individuals is the case of John Catt, a pensioner who found that his car had been 'marked' by the police ANPR system. Following his attendance at peace demonstrations near Brighton he was regularly stopped and questioned by police under anti-terrorism legislation.[16]

116 **Key Finding**: In general the presence of CCTV cameras in public spaces is not seen as an intrusion into privacy. However, new technologies have increased the scope and processing capabilities of camera surveillance and are often assembled in a piecemeal way without citizens being aware of their implications. Too much surveillance can fundamentally alter the relationship between the individual and the State.

Public engagement

117 In order to retain public confidence in the appropriate use of CCTV in public spaces it is essential that the States of Jersey Police and other public sector CCTV operators engage with the public in an open and transparent way to explain the capabilities and limitations of their systems.

118 Our advisors noted in their interim report following the first set of interviews and site visits conducted in early May 2013: 'The ongoing provision of CCTV is dependent upon public support for systems. CCTV is controversial because it captures personal data and because it shapes behaviour (it has been designated by the European Parliament as a 'tool of social and political control'). It is important therefore that service providers and CCTV operators make the public aware of the existence and use of CCTV. This is a basic requirement in other parts of Europe. This can be achieved in a number of ways

[15] Public hearing 26.06.13, page
[16] http://www.theguardian.com/uk/2013/jun/25/undercover-police-domestic-extremism-unit

and is particularly pertinent for those being surveyed. The requirement for public engagement could be embedded in a Code of Practice.'

119 Public engagement should occur in the following instances:

- via appropriate signage,
- consultation on camera location, especially in the case of new cameras or an expansion to an existing system (including links to new databases), and
- direct engagement with those domestic properties within view of the surveillance camera (this should include an invitation to visit the control room). This would also include parents at schools.

120 Currently, the main town centre system in St Helier does not have any public signage. In this respect, the public do not know that the systems is a 'police' system used for operation issues, or who to contact in relation to the operation of the system and the processing of personal data. This is contrary to normal practice elsewhere in the UK.

121 The Information Commissioner's Code of Practice (2008) contains sections on signage and how to effectively advertise the existence of CCTV surveillance in a given area. Signs should be visible and readable, contain details of the organization operating the system, the purpose of operating CCTV and who to contact about the scheme.[17]

122 We noted that many local authorities in the UK provide the public with extensive information about public space CCTV camera systems. Cambridge City Council, for example, provides a range of relevant information and documents including an Overview providing details of the location and arc of observation for 139 cameras within the city centre and its car parks[18]. This compares to a single page on the States of Jersey Police website[19] which provides only general advice on the siting and use of CCTV but no information on cameras operated by the States of Jersey Police in the Town Centre.

123 We asked the States of Jersey Police whether there was any operational reason why information on the location of cameras should not be made publicly available. This is

[17] Chapter 9 Responsibilities
[18] https://www.cambridge.gov.uk/cctv
[19] https://www.jersey.police.uk/crime/HomeandBelongings/Pages/CCTV.aspx

a basic requirement in the UK and is in accordance with the Information Commissioner's Code of Practice. Acting Chief Inspector Williamson said that there was no intention of secrecy in the siting of cameras; however signage had not been considered necessary as the units were very visible and everyone knew that there were cameras in place.

124 He said that specific information on locations had been provided in a press release at the time of the initial introduction of CCTV in St Helier, when public interest had been high and again in 2001 and 2006 when the network of cameras had been increased.

125 He told us that, in the early days of CCTV, the States of Jersey Police had introduced a system to routinely capture and publish data relating to the use and number of incidents recorded via the town CCTV system. In essence, the Force Control Room officers were required to endorse all individual incident reports (i-logs) whether CCTV had been utilised or played a part in an arrest. This information was utilised to assess some of the impact of CCTV and inform the public.

126 The 2006 States of Jersey Police Performance Report stated that Town CCTV cameras actively monitored 2,035 incidents requiring police action, leading to the arrest of 437 offenders. Such data has not been routinely utilised since 2006. The Police had believed that the benefits of CCTV had been well established in the public mind by this time and it was no longer necessary to make a continuing case for their use.

127 **Key Finding**: The States of Jersey Police currently provide minimal information to the public on the Town Centre CCTV system, the location of cameras and its operational procedures. Performance reporting which used to be included in States of Jersey Police Annual reports has been discontinued.

128 **Recommendation**: The States of Jersey Police should follow the example of local authorities in the UK and provide extensive information on their website on the Town Centre CCTV system including a map indicating the location of cameras.

129 **Recommendation**: Appropriate signage should be erected in the town centre indicating that CCTV surveillance is taking place with a contact point for members of the public with queries.

10 The effectiveness and impacts of camera surveillance

The role played by camera surveillance in policing, community safety, transport and the criminal justice system

130 **Policing:** The States of Jersey Policing Plan 2013 states that CCTV 'is an essential tool in protecting public safety and security through the effective deployment of Police resources. Where CCTV is available:

- Police resources are deployed where they are needed most, thereby making optimum use of available capacity to protect community safety
- Police can make swift, appropriate deployments and attending officers have prior knowledge of what has occurred, who is involved and their current location;
- Camera footage can help secure the swift conviction of offenders, thereby reducing costs associated with the investigation and prosecution processes.

131 **Criminal Justice System**: The Minister for Home Affairs told us that he was very positive about the benefits of CCTV within the criminal justice system: '*From the standpoint of a former Magistrate*', he said, '*the evidential value was massive, both in terms of proving the prosecution case but sometimes in terms of proving the defence case because it does have this element of objectivity*'[20].

132 The Judicial Greffe and Magistrate's Court Greffe added that CCTV was capable of providing objective evidence of an incident whereas a witness' recall might be partial or confused. CCTV was generally used within the criminal justice system as part of corroborative evidence to show a person's movements in the vicinity of an incident. It could also be used to provide the context for an incident, for example CCTV was used by the defendant in the Royal Court in a recent assault case to demonstrate that his actions were not as serious as had been alleged. In some cases CCTV may be critical to the outcome of a case. Generally however it is only part of the evidence provided by the prosecution.

[20] Public hearing, 28.06.13, page 2

133 **Community safety**: An example of the use of CCTV to enhance community safety was provided by the Housing Department in its Community Newsletter in 2006. The Department compared the amount of complaints relating to anti-social behaviour from five large family estates with CCTV compared with five similar estates without CCTV and found 26 complaints in the former compared to 45 in the latter. They concluded that this showed that CCTV could work as a deterrent and reduce reports of anti-social behaviour by a significant amount[21].

134 In response to a request for further detail on how CCTV had been used to assist with investigations into anti-social behaviour on Housing estates the department provided the following information:

> *In 2012 there were 8 requests by the Police to review our CCTV regarding incidents they were investigating, 4 were positive results, and 4 negative results.*
> *In 2013 there were 13 requests by the police to review our CCTV regarding incidents they were investigating, 12 were positive results, and one was a negative result.*
> *Apart from the above we do receive requests from our contractors and residents regarding incidents, however these are not recorded separately as if there is any CCTV footage the incident is reported directly to the Police as a complaint.*
> *This year there was one request from one of our contractors that led to a positive result, and two from our residents - one positive and the other negative.*

135 A respondent to our online survey also saw CCTV as an answer to community safety worries on a housing estate: '*I would like to see moveable, flexible solutions to CCTV as well as being able to monitor key areas. For instance we had a problem with our neighbours and with cars driving through our (Housing Trust) estate and for our own safety. The Housing Trust have not responded to the request for signs encouraging safe, slow driving or signs that alert drivers to children playing. They have also not been able to mention anything about antisocial and sometimes aggressive behaviour of my neighbours leaving the only option open to us as the police. In particular the police*

[21] Community News, States of Jersey Housing, issue 6, August 2006

cannot do anything about traffic offences within our estate as it is a private area apparently (a poor excuse from all I think). CCTV on even a temporary measure would help deter inappropriate behaviour and driving before a child or other person gets seriously hurt. It would also deter other anti-social activities and ultimately could provide evidence if need be on how a neighbourhood 'community' dynamic could be improved. Doing this as a neighbour won't send out the best cohesive message, but a third party ability would.'

136 CCTV cameras have been erected by private organisations in public areas, for example Les Quennevais Precinct car park and Bonne Nuit Harbour, in response to incidents of malicious damage.

137 **Car parks**: Research into the effectiveness of CCTV cameras referred to below[22] has found that CCTV is most effective in reducing crime in car parks. All multi-storey car parks in St Helier together with two surface car parks, the Esplanade and Snow Hill, are monitored by CCTV cameras. Two privately operated car parks at the Waterfront and Kensington Place also operate CCTV systems. In Jersey their principal uses are to monitor illegal parking and overstaying and are used to ensure smooth traffic flows. CCTV footage is sometimes requested by members of the public in relation to insurance claims for accidental damage.

138 **Transport:** CCTV surveillance is a common feature in all forms of transport, especially internationally. CCTV cameras at the Airport and Harbour are essential to meet national and international security requirements. Cameras are also becoming increasingly visible in our buses and taxis.

139 **Bus travel**: The General Director, Liberty Bus, told us that CCTV cameras installed on their buses had improved the security of passengers, particularly on night time services where it was no longer necessary to provide additional security presence.

140 **Taxis:** A number of taxi drivers in Jersey are now fitting their vehicles with CCTV cameras in order to improve their protection from assault by passengers. Others are

[22] Campbell Collaboration Report, Dec 2008 – see paragraph 134

opposed to this development on the grounds that the taxi space is considered a private area by customers.

Evidence for the effectiveness of camera surveillance in preventing and detecting crime and promoting public safety

141 There is an overwhelming view among operators that CCTV provides a vital function in enhancing public safety and reducing crime and disorder in Jersey. Many witnesses, including the States of Jersey Police and the Magistrate's Court, gave us anecdotal evidence, demonstrating the impact of CCTV in the efficient use of police resources and gains in reducing court proceedings, but robust evidence, backed by statistical data, for the reduction and prevention of crime is hard to find.

Research: Campbell Collaboration

142 There is an ongoing debate across Europe about the effectiveness of CCTV. In December 2008 a report was published by the Campbell Collaboration which examined a range of studies looking at scientific evidence for the effects of CCTV on crime. The report focused on CCTV in public space where the prevention or personal and property crime was among the primary objectives. The main objective of this review was to assess the available research evidence on the effects of CCTV surveillance cameras on crime in public space. In addition to assessing the overall impact of CCTV on crime, this review also investigated in which settings (e.g., city and town centres, car parks), against which crimes, and under what conditions it was most effective.

143 The reviewers noted that CCTV was the single most heavily funded crime prevention measure operating outside of the criminal justice system. It accounted for more than three-quarters of total spending on crime prevention by the British Home Office. The authors called for more high-quality research on the topic in order to demonstrate whether such large sums of money had been well spent*: In recent years, there has been a marked and sustained growth in the use of CCTV surveillance cameras to prevent crime in public places in many Western nations. This growth in CCTV has come with a huge price tag. In the U.K., CCTV continues to be the single most heavily funded crime prevention measure operating outside of the criminal justice system. It is*

estimated that more than £250 million (approximately $500 million) of public money was spent on CCTV over the ten-year period of 1992 to 2002. This figure could very well be an underestimate. For example, between 1999 and 2001 alone, the British government made available £170 million (approximately $340 million) for "CCTV schemes in town and city centres, car parks, crime hot-spots and residential areas". Over the last decade, CCTV accounted for more than three-quarters of total spending on crime prevention by the British Home Office.[23]

144 In giving the background to this review the reviewers noted the lack of high quality independent research into the impact and effectiveness of CCTV: *A key issue is how far funding for CCTV in the U.K. has been based on high quality scientific evidence demonstrating its efficacy in preventing crime. There is concern that this funding has been* based *partly on a handful of apparently successful schemes that were usually evaluated using simple one group (no control group) before-after designs, done with varying degrees of competence, and done with varying degrees of professional independence from the Home Office. Recent reviews that have examined the effectiveness of CCTV against crime have also noted the need for high quality, independent evaluation research.*[24]

145 The reviewers considered a number of views which are commonly held regarding the impact of CCTV on crime including:

- Potential offenders being deterred by an increased perception that their actions would be detected;
- Increased use by pedestrians of the areas under surveillance by CCTV leading to an increased probability of detection;
- Potential victims being encouraged to take additional security precautions
- Police and security personnel being directed to intervene
- CCTV signalling improvements in the area and hence increasing community pride, community cohesion, and informal social control;
- CCTV encouraging increased reporting of crimes to the police

[23] Campbell Collaboration report, Dec 2008, page 4
[24] Ibid page 4

- CCTV in combination with other interventions such as improved street lighting.
- CCTV causing crime to increase, for example by giving potential victims a false sense of security.
- CCTV causing crime to be displaced to other locations, times or victims.

146 In its conclusion the Campbell Collaboration report described the effect of CCTV on crime as '*modest but significant'*. '*CCTV … is most effective in reducing crime in car parks, is most effective when targeted at vehicle crimes (largely a function of the successful car park schemes), and is more effective in reducing crime in the United Kingdom than in other countries*[25].

147 The reviewers suggested that, in contrast to its current broad application, CCTV usage should be focused only on the specific targets against which it is shown to be most effective '*It is plausible to suggest that CCTV schemes with high coverage and other interventions and targeted on vehicle crimes are effective. Conversely, the evaluations of CCTV schemes in city and town centers and public housing measured a much larger range of crime types and only a small number of studies involved other interventions. These CCTV schemes, as well as those focused on public transport, did not have a significant effect on crime*.'[26]

Metropolitan Police Report

148 Doubts about the effectiveness of CCTV were raised by a Metropolitan Police report in 2009 which warned that the police had to work harder to improve the use of CCTV in the fight against crime to give the public confidence in the use of CCTV. The report noted that there were more than one million CCTV cameras in London and the government had spent £500m on the equipment; but in 2008 only 1,000 crimes were solved using CCTV images because officers failed to make the most of potentially vital evidence.

[25] Ibid, page 18
[26] Ibid page 19

149 The report said that people were filmed many times every day and had high expectations when they became victims of crime but suggested that the reality was often disappointing as, in some cases, officers did not bring criminals to justice even after they were caught on camera and identified. CCTV played a role in capturing just eight out of 269 suspected robberies across London in one month.

150 Detective Chief Inspector Neville, the author of the report, is leading a scheme aimed at making the investigation of CCTV evidence as professional as fingerprinting and DNA technology[27].

NO-CCTV

151 Mr. Farrier said that decisions installing or extending CCTV should be based on evidence. If the States of Jersey Police genuinely believed cameras performed as they claimed, why, he asked, would they not provide evidence to support this? Relevant information should include:

(i) the number of arrests actually made as a result of CCTV evidence,
(ii) the number of cases proceeding to prosecutions
(iii) what form of intervention was actually played by CCTV (for example whether it was a contributing factor or essential factor)
(iv) whether prosecution cases were successful or not
(v) whether CCTV actually assisted with early guilty pleas.

152 Mr. Farrier said: *When you did have the police giving evidence, they were talking about collecting* the *figures for a while and then not collecting figures, that they had neglected those. I would urge them to collect those figures again but to break them down in a more detailed way, to look at how often are the cameras used, what are they used for, how many of those cases go to court and in those cases to what degree can we track that through and see it moving forward. I am sure nowadays the ability to track this stuff is easier than it once was because, as I say, so much is digital anyway*[28].

[27] http://www.independent.co.uk/news/uk/crime/cctv-in-the-spotlight-one-crime-solved-for-every-1000-cameras-1776774.html
[28] Public hearing 18.09.13, page 8

153 Mr. Farrier claimed that the benefits of CCTV had been overstated by the UK Home Office to boost the false image that cameras are effective and to support the huge investment in camera technology. However, he said, all studies to date conclude that cameras are not effective. [29]

154 In his written submission Mr. Farrier criticised the way in which the UK government had handled the Campbell Collaboration report which had systematically examined research into the effectiveness of CCTV because they chose to quote extensively from the synopsis of the report misleadingly using the word 'crime' instead of 'car crime' .

155 Mr. Farrier pointed out that, contrary to general perception, CCTV did not provide incontrovertible evidence for events. CCTV is presented in court, he said, as some form of forensic evidence; however, this was not the case. 'I think that the problem with the way that C.C.T.V. evidence is introduced into courts is that it is presented as though it was some sort of forensic evidence, that it was the same as forensics. The problem is we have an adversarial court system and there is no challenge on C.C.T.V. We often hear people saying that C.C.T.V. proves that we can see what is happening but, you know, it is in the eye of the beholder. We have criminal defence solicitors that we talk to at No CCTV who will tell us that they have seen C.C.T.V. played where defence solicitors have said: "That clearly shows my client not attacking somebody" and the police say: "That clearly shows your defendant attacking somebody" but there is no real way of challenging that evidence. If fingerprint evidence is produced in court, that is forensic evidence, you bring in an expert, the expert can be challenged in the adversarial system. C.C.T.V. is not and that is a problem in the court system, I think.'

156 Mr. Farrier said that the public were too easily persuaded about the effectiveness of CCTV. When asked how to shift that kind of opinion, he replied:

> *I think by some honesty from politicians and honesty about the figures and the scale of what is really happening here, for people to understand ... If you talk to policemen, they will often say it is not a silver bullet, it does not do everything. It is not superb, it does not solve all the world's problems, but an awful lot of the*

[29] Ibid page 5

general public think it does. If you talk to members of the public about C.C.T.V., they will want more cameras, more cameras, more cameras. Why do they want more cameras? Because they think it works. So they have got unrealistic expectations of cameras.[30]

157 In his written submission Mr. Farrier suggested that the following questions should be the starting point for any discussion regarding surveillance technology:

- What is the problem to which this technology is the solution?
- Whose problem is it?
- What new problems might be created by solving the original problem?
- What other less intrusive solutions have you tried?
- Do you have proof that cameras will assist?
- How will you measure the success or failure of the cameras?
- If the cameras do not assist how long will it be before you take them down?[31]

Jersey Human Rights Group

158 In a submission to our review the Jersey Human Rights Group (JHRG) stated that they had real concern that public support for police CCTV was based on a false impression of effectiveness. In their view the position of Home Affairs and the States of Jersey Police appeared to be from the evidence given in the public hearings: '*CCTV has been in extensive use, both in the UK and Jersey for several years without generating any problems. The public do not complain about it; on the contrary it provides the public with a sense of security. We do not have to worry about it anymore*.'[32]

159 The JHRG called for a study to address the following broad questions of whether state surveillance is generally:

- Socially beneficial, ie reduces crime and /or improves the solving and conviction of crimes

[30] Ibid
[31] No-CCTV Submission, para 59, based on questions posed by Neil Postman, Technology and Society lecture, Calvin College, 1998
[32] http://www.scrutiny.gov.je/Pages/Review.aspx?ReviewId=185

- Risky, because of the additional power and knowledge that it gives the States; and the related question of how it should be regulated and by whom;
- Cost effective (or to put it another way – could the resources consumed by CCTV be used more effectively in other ways); or
- Undesirable because of the inevitable loss of privacy33

160 We trust that our review, together with the contribution of our advisers, goes some way to address the above questions; albeit in our view there can be no definitive or simple answer to the issues raised by the JHRG which have been the subject of numerous academic studies. Reference is made in Appendix 3 of this report for the interested reader to a number of key documents relating to operation, standards and data handling in relation to CCTV published by local authorities, national government and the private sector.

Evaluation mechanisms

161 Our advisers highlighted the problem of the lack of mechanisms in the Jersey public sector to monitor the long-term effectiveness of cameras: 'During one public hearing the States of Jersey Police representative argued that it would be 'too expensive' to monitor the effectiveness of cameras. It would also be possible to argue that simple evaluation could prove less expensive than new inappropriately or ineffectively sited camera installations. Moreover, if understanding of the uses of CCTV is limited, then it would follow that knowledge over the extent to which systems are used properly is also restricted.

162 In other domains, notably education, once budgets have been devolved to their discretionary holders there appears to be little reflection on how surveillance cameras are operated nor any analysis of their efficacy. If the cameras are not proven to be offering security then, arguably, incursions into privacy become less justifiable.

[33] Ibid

163 They concluded: 'We accept that evaluation processes may be complex and onerous but, equally, some simple measures could be introduced to improve this situation. Given this lack of analysis, the police controlled CCTV system does not meet the requirements laid out in Jersey's CCTV Code of Practice and cannot be said to be fully compliant in this regard.'[34]

164 The advisers made the following suggestions: 'Part of the problem, is that CCTV has multiple purposes and is just as useful in directing police resources as it is in deterring and detecting crime. For this reason, we suggest that CCTV data controllers are very specific about the purpose of systems. If they are more specific about the purpose of systems then these systems become easier to audit and evaluate and political accountability and oversight can be achieved.

165 The new Data Protection Directive being developed by the European Commission is likely to incorporate a requirement for 'purpose limitation', which implies that a system introduced for one purpose should not then be used for another. With this in mind, statements about purpose and objectives are critical if systems are to be compliant with future European and national legislation.[35]

166 The evaluation or audit of the performance and effectiveness of camera systems should be undertaken periodically and not less than once a year. A series of performance indicators should be established which relate to the purpose of the camera system (as specified by the Data Controller). Evaluations should include, but are not restricted to:

- The frequency and types of offence captured.
- The number of requests to review footage (and when and by whom).
- Whether footage was used in the prosecution.
- How many times the control room was visited (and when and by whom).
- The number of times targeted surveillance took place (where individuals were followed for longer than the agreed time period).

[34] Initial thoughts on first two visits, 30 August 2013, Professors P. Fussey and W. Webster
[35] Impressions and recommendations from initial visit to Jersey May 2013, Professors P. Fussey and W. Webster

- An analysis of crime statistics in surveyed areas.
- The results of consultation undertaken during the review period.
- Operator training completed.
- Auditable processes to demonstrate management checks on surveillance practices.
- Frequency of inoperative cameras and other equipment.
- Log of citizen requests for information.
- Auditable process to demonstrate compliance with the Data protection Commissioners CCTV Code of Practice.

167 **Key Finding**: There is a tendency, once a system has been in operation for some time, to assume that the purposes and benefits of a system are understood and accepted and therefore to neglect the importance of keeping the public fully informed. Public sector CCTV operators in Jersey, particularly the States of Jersey Police who are responsible for the Town Centre CCTV network, should ensure that they provide the public with a regular analysis of the efficacy of their systems. The introduction of a new Town Centre CCTV system sharpens the focus on the need for the States of Jersey Police to provide the public with a good business case demonstrating value for money for the project.

168 **Recommendation:** All States departments operating 'public' CCTV systems should undertake an annual review/audit, which sets out the scope of the system, its stated purpose(s) and a range of performance indicators which can be utilised to judge the effectiveness of the system (see paragraph 166 above).

169 **Recommendation:** We also recommend including some comparison of the crime rates in areas observed by CCTV against those without coverage in order to assist understandings of crime displacement and to provide and evidence base to inform future camera deployment decisions. This process should be followed by a review of the appropriateness of existing camera positioning.

11 The governance of cameras surveillance

The effectiveness of current guidelines/voluntary codes of best practice and their operation

171 The Data Protection Commissioner told us that the *Code of Practice and Guidance on the Use of CCTV* published by her office in 2005 was issued because they had seen an increase in both the use and the number of enquiries coming to them. The Code of Practice provides a framework around the use of CCTV images in accordance with general data protection principles.

172 She explained that the basic principles applied to CCTV notwithstanding the advances of technology; they also applied even where an operator has failed to register a CCTV system. She elaborated on these principles:

- Transparency: This means being clear about who is operating the system, and what they are doing with the data; through signage, staff handbooks, published policies; in relation to CCTV in the workplace it's about having a dialogue with staff about the purpose of cameras so that they understand the problem their employer is trying to address through CCTV;
- Fairness of processing: This requires purpose limitation: being clear upfront about the purpose of CCTV systems; not using CCTV footage for purposes other than those stated;
- Proportionality of processing: This means using CCTV only in response to a real, identified need;
- Security of data: This means clarity about what happens with CCTV images, who has access, where they are stored, how they are deleted;
- Retention of data: CCTV images should be deleted after a set period of time. The Code is not prescriptive on this issue: the length of time images are retained may depend on who is collecting and why;
- Access to data: CCTV images may be legitimately disclosed to the police for crime prevention. There should be an audit trail for anyone who has access to data; images should not be passed on to third parties (eg YouTube); the data controller is responsible for passing on correctly. Subject access rights to information held on individuals should be clearly defined.

Codes of Practice

Data Protection Code of Practice and Guidance on the Use of CCTV

173 Standard procedures for viewing, recording, retention and processing of data captured on CCTV are set out in the *Data Protection Code of Practice and Guidance on the Use of CCTV (2005) ('The Code')*. This Code elaborates on the implications of the Data Protection (Jersey) Law 2005 for operators of CCTV systems and is modelled on the Codes of Practice issued by the UK Home Office and Information Commissioner.[36]

174 The Code deals with surveillance in areas to which the public have free and unrestricted access. It explains the legal obligations for CCTV operators under the Data Protection (Jersey) Law 2005, describes best practice and provides reassurance for the public about the safeguards that should be in place.

175 The Code does not apply to:

- Targeted and intrusive surveillance activities which are covered by the provisions of the Regulation of Investigatory Powers (Jersey) Law 2005
- Use of surveillance techniques by employers to monitor their employees' compliance with their contracts of employment
- Security equipment (including cameras) installed in homes by individuals for home security purposes
- Use of cameras and similar equipment by the broadcast media for the purposes of journalism, or for artistic or literary purposes37

176 The Code requires operators to assess reasons for the installation of CCTV, establish and document the purposes of the scheme, persons responsible for the operation of the scheme and its compliance with the Code, their security and disclosure policies. CCTV schemes should be registered with the Data Protection Commissioner.

177 The Code requires that operators ensure that

[36] The latest UK government guidance on CCTV operational practice was issued in June 2013. The principles of this guidance are discussed elsewhere in this report
[37] Code of Practice and Guidance on the use of CCTV, Data Protection Commissioner, 2005

- access to recorded images should be restricted to managers or designated members of staff
- there should be an audit trail for the removal of recorded images from the system
- operators should be trained in their responsibilities under the scheme
- standard subject access forms should be available on request to members of the public
- signs should be placed so that the public are aware that they are entering a zone covered by surveillance equipment.

178 **Key Finding**: Every CCTV operator should have their own publicly available code of practice compliant with the Data Commissioner's *Code of Practice and Guidance in the Use of CCTV* setting out the purpose of the system, their data management procedures and security policies and their training processes for CCTV operators. This Code of Practice should be reviewed on a regular basis to ensure that the CCTV system is operating effectively against stated purposes.

Public sector

179 The Data Protection Commissioner told us that it was particularly important for public sector bodies to have fair and transparent policies in place and demonstrate the highest standards of compliance with data protection principles as interaction with the public service by its citizens is 'very infrequently voluntary'[38]. She said that every States department had designated data protection officers in place. She found that States Departments were generally proactive in engaging with her office at an early stage whenever new systems were installed, for example the trial ANPR system at Sand Street car park linked to a new payment system and the States of Jersey Police trial for the use of body-worn cameras where good policies had been established for the appropriate use of CCTV[39].

180 Our survey of States Departments indicated however that not all departments had their own code of practice. The Prison and Transport and Technical Services, except for

[38] Public hearing 26.06.13, pages 23 & 52
[39] Ibid page 49

the Car parks section, for example, simply referred to the *Data Protection Code of Practice* as the model. Transport and Technical Services use of CCTV was largely focused on site and process operations at installations where the public had limited access (eg Energy from Waste plant, Bellozanne and the abattoir site).

181 In contrast the car parks section of Transport and Technical Services had recently created its own internal document following discussions with the Commissioner around the new ANPR system. We found that Housing had its own detailed and specific code of practice.

182 The Department for Education Sport and Culture told us that each school, college or sports centre which operated CCTV systems was individually responsible for the data management of their systems. The person responsible is generally the head teacher, network manager or site manager. As previously stated most schools use CCTV only for external security and not for monitoring pupils. We are not aware of any schools which have their own specific policies on CCTV usage.

183 We found a surprising lack of compliance with one particular aspect of security across a number of departments. We visited a number of CCTV suites in States departments, including the States of Jersey Police, the Jersey Customs and Immigration Service, Airport Security, Transport and Technical Services Car Parks. There appeared to be no register of access to any of these suites contrary to standard practice elsewhere in Europe.

184 **Key Finding**: There is inconsistency across States departments in relation to compliance with the requirement for all CCTV operators to have their own Code of Practice – a number refer simply to the *Data Protection Code of Practice and Guidance in the Use of CCTV* as their model whereas it should be standard practice for all public sector CCTV operators to have a specific code of practice for their operation.

185 **Recommendation**: All States departments using CCTV should have their own dedicated and publicly available code of practice setting out their purpose, data management procedures, security policies and training procedures as well as information to the public on how they can contact the organisation in case of queries about their

operation of CCTV. All public sector CCTV operators should be required to have a log of who has had training and when.

States of Jersey Police

186 It is particularly important for the Police CCTV operators to have robust procedures respecting the privacy of individuals who may be observed. Misuse of the system would undermine public trust in the appropriate use of systems. In Jersey, because of the small population, there is a very high likelihood that CCTV operators will recognise subjects throughout any given shift.

187 The Data Protection Commissioner said that she was confident that the Police understood standard procedures and policies for CCTV usage. Compliance was essential for the provision of good quality images required for evidence in court and the Police were increasingly aware of the consequences for prosecution cases in not following procedures.

188 Signage in the Force Control room states three key rationales for which the recording and retention of images are authorised: monitoring for potential criminal activity, investigating criminal activity, providing evidence of such activity in legal proceedings.

189 Force Control Room officers (uniform and civilian staff assisted by Honorary officers) are in principle the only ones with access to the CCTV control room (except for specific reasons such as training or visits).

190 Training in the operation of CCTV is included within the training programme for Force Control Room staff. It is essential that any public agency operating CCTV in a public space should provide operators with training related to data processing and privacy issues. The States of Jersey Police Force requires its Force Room Control staff to undergo a seven day programme of which two days are devoted to CCTV techniques and Data Protection principles.

191 The States of Jersey Police provided us with copies of their Code of Practice and Town Centre CCTV Force policy. We noted that both documents were over ten years' old and contained references to outdated technology. More importantly, certain aspects

of good practice were no longer active, for example, the production of an annual report on the impact of the scheme and regular evaluation of its effectiveness. We were told that these were no longer considered necessary as the public understood and accepted the benefits of CCTV[40].

192 Our advisers commented: 'The current operation of CCTV by the States of Jersey Police falls short of what is seen elsewhere in the UK and Europe, both in terms of 'day to day' operation and the governance of systems. Consequently, it is difficult to be confident that the police use of CCTV is appropriate, justified or fair (this is not to say that systems are misused by the Police). Updated practices are likely to result in greater public confidence in the Police use of CCTV. We would suggest that this is vitally important for the ongoing provision of CCTV in Jersey and should be a necessary requirement before the States of Jersey police are allowed to expand and digitise systems.'[41]

193 **Key Finding:** Training related to data processing and privacy principles is an essential element in the training programme for States of Jersey Police Force CCTV operators. However, the current Police Code of Practice falls short of what is seen elsewhere in the UK and Europe. The Police have acknowledged the requirement to update their policies and procedures and have assured the Panel that the documents would be reviewed as part of their project to renew and extend the current Town Centre system.

194 **Recommendation:** Appropriate governance arrangements, an updated Code of Practice, and the introduction of auditable process should be introduced as a matter of urgency to ensure the delivery of a service in the public interest and to ensure compliance with UK and European standards and norms in the provision of CCTV.

Commercial sector

195 Many of the stipulations of the Code of Practice are not strict legal requirements for businesses but represent the following of best practice. The Data Protection

[40] Public hearing 26.06.13 page 26
[41] Initial thoughts on visits

Commissioner commented that, although this document does not have the force of statutory regulation it would be difficult to envisage that a business was compliant with the law if it did not comply with the Code.

196 The main CCTV installers, which are certified by the SSIAB, advise their customers about data protection obligations.

197 The Data Protection Commissioner said that her office worked hard to ensure that businesses were aware of their responsibilities[42]. Many companies, particularly those who are part of large UK companies, had their own formal codes of practice; however, this was far from normal practice. She said that it was often a challenge to engage with smaller companies who might find data protection issues overwhelming. The approach taken by her office was pragmatic: most companies were willing to comply with best practice but might need reminders (for example about the lack of signage) or make mistakes (for example about unfair collection of data for purposes different to those stated in their registration).

Developments in Governance

198 Since the publication of this Code of Practice in 2005 there have been a number of important developments in the UK in the governance and regulation of CCTV.

National CCTV Strategy, Home Office, October 2007[43]

199 This was the first attempt at creating a national coordinated approach to the operation of CCTV. The strategy was authored by the Home Office (National Police Improvement Agency) and ACPO. The emphasis here is the standardisation of technologies and administrative processes in order to maximise the effectiveness of systems. Whilst some recommendations have been superseded by the 2013 Home Office Code of Practice, the National Strategy sets out a number of clear principles for the operation of CCTV.

[42] Public hearing 26.06.13 page 11
[43] http://www.statewatch.org/news/2007/nov/uk-national-cctv-strategy.pdf

200 The information on the retention of data is particularly relevant for Jersey. The standard maximum length of time for retaining CCTV images before recording over is between 28 and 31 days. Since the introduction of digital CCTV systems, some systems owners have moved from the 28 to 31 days figure to periods as short as 14 days.[44] Personal data captured by CCTV is stored for varying lengths of time across different organisations using CCTV in Jersey. In almost all cases, the length of time exceeds that governing data retention in the UK and elsewhere in Europe.

201 **Key Finding:** Some CCTV operators, particularly the police, have articulated a reason for lengthy retention periods. However, a case needs to be made for why the Police and other operators require much longer periods of data retention (sometimes triple) than, say, London's Metropolitan Police, given the significantly lower levels of crime and disorder in Jersey.

202 **Recommendation:** The *Data Protection Code of Practice and Guidance on the Use of CCTV* should specify standardised retention periods based on the operational purposes of the CCTV systems.

203 **Recommendation:** The States of Jersey Police, as part of updating their code of practice and procedures on CCTV, should review their policy on retention periods to ensure that they are in line with current best practice.

UK Information Commissioner's Office (ICO) Code of Practice (2008)[45]

204 This Code updated an earlier Code of Practice issued by the Information Commissioner's office in 2000. It was based on discussions with organisations that use CCTV and a public consultation exercise and took account of advances in the way CCTV is used, the technology employed and 'developments which might help achieve more privacy friendly ways of using CCTV'.

[44] National CCTV Strategy, Home Office, October 2007, chapter 6
[45] http://www.ico.org.uk/for_organisations/data_protection/topic_guides/~/media/documents/library/Data_Protection/Detailed_specialist_guides/ICO_CCTVFINAL_2301.pdf

205 The Code places the issue of privacy at the forefront of decision making on whether organisations should use or continue to use CCTV: '*You should carefully consider whether to use it; the fact that it is possible, affordable or has public support should not be the primary motivating factor. You should take into account what benefits can be gained, whether better solutions exist, and what effect it may have on individuals*.'[46]

206 The Code advises organisations to review regularly whether the use of CCTV continues to be justified. The annual notification is the appropriate time to consider the ongoing use of CCTV.

207 The Jersey Data Protection Commissioner's Code of Practice includes advice for CCTV operators to undertake an internal annual assessment which evaluates the effectiveness of the system against the stated purpose of the scheme. The Code states that if the scheme is not achieving its purpose it should be discontinued or modified. The Code also includes advice on maintaining the quality of images in order to ensure that images are effective for the purposes(s) for which they were intended.[47]

208 **Key Finding:** We have seen little evidence that effective reviews of CCTV systems actually take place in the public sector. We are not aware of any systems which have been discontinued if they are found not to be achieving their stated purpose.

209 **Recommendation**: The requirement that public sector CCTV operators should undertake a minimum standard of evaluation on an annual basis to ensure that their systems are effective and appropriately sited should be reinforced. This evaluation should be included in annual returns to the Data Protection Commissioner.

Home Office Surveillance Camera Code of Practice (June 2013)[48]

210 This is the latest UK government guidance on CCTV operational practice. It only applies to public bodies but the main principles could be embedded into the activities of

[46] Chapter 4 Deciding whether to use CCTV or continue using CCTV
[47] Code of Practice, pages 18 and 10
[48] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/204775/Surveillance_Camera_Code_of_Practice_WEB.pdf

private operators. There is considerable emphasis placed on accountability, transparency and responsibility – all areas that are relevant to Jersey.

211 The most relevant section of the new Code concerns the notion of 'surveillance by consent'. *The government considers that wherever overt surveillance in public places is in pursuit of a legitimate aim and meets a pressing need, any such surveillance should be characterised as surveillance by consent, and such consent on the part of the community must be informed consent and not assumed by a system operator*[49].

212 This notion of 'surveillance by consent' is analogous to 'policing by consent': *In the British* model *of policing, police officers are citizens in uniform. They exercise their powers to police their fellow citizens with the implicit consent of their fellow citizens. Policing by consent is the phrase used to describe this. It denotes that the legitimacy of policing in the eyes of the public is based upon a general consensus of support that follows from transparency about their powers, demonstrating integrity in exercising those powers and their accountability for doing so.*[50]

213 Charles Farrier, co-founder of No-CCTV, criticised the concept of 'surveillance by consent' as merely a catchphrase. He said that consent in law was something that is freely given and can be removed: '*The idea of informed consent would involve education of the public into what really cameras are doing. That would be quite a job, but I would like to see that, I would like to see the public more aware of the realities of cameras*.[51]

214 Mr. Farrier said that the notion of 'surveillance by consent' which was used now to legitimise ongoing monitoring in public places was difficult: '*it becomes very tricky with C.C.T.V.* cameras *and they always talk about implied consent which is that, because you have agreed to get on a bus, you have consented to being under surveillance. But if there are no buses without surveillance and you want to get a bus, it is very difficult to see how you did consent, and there is no model for you to get on that bus and say: "I*

[49] Home Office: Surveillance Code of Practice, para 1.5
[50] Ibid
[51] Public hearing, 18.09.13, page 15

would like to get your bus, please, but honestly I do not consent to your surveillance" and that is a tricky thing and it has not been dealt with.[52]

215 Our advisers commented on this issue: 'Surveillance by consent is becoming a key element of CCTV practice in the UK and EU. We have not encountered any initiatives that seek to understand the extent to which surveillance operates on a consensual basis in Jersey. Statements such as 'everyone recognizes the benefits' of CCTV are often expressed, and may be true, but no evidence has been offered to support such sentiments. Genuine public engagement should be a cornerstone of achieving surveillance by consent. A simple well-designed and infrequently administered survey could be one way of working towards this aim. If public approval is proven to be as high as practitioners imagine, then such evidence would also give them a robust mandate for their activities. We would expect public engagement to be an element of the States of Jersey Police CCTV Code of Practice.

216 **Recommendation**: The *Data Protection Code of Practice and Guidance on the use of CCTV* should incorporate a legal requirement to comply with the principles of surveillance by consent, including a requirement for signage, consultation and public awareness mechanisms.

217 **Recommendation**: The Code of Practice should also contain a requirement for all CCTV operators to make the public aware of the location of cameras, the purpose of systems and any data matching that may take place.

218 **Key Finding**: In view of the above developments it is apparent that some aspects of Jersey's *Data* Protection *Code of Practice and Guidance in the Use of CCTV* are outdated and should be brought in line with best practice elsewhere in the UK and Europe. Our advisers have made a number of suggestions for areas of improvement in the existing Code of Practice. (see appendix)

219 We asked the Data Protection Commissioner about updating the Code of Practice. She said that her office acknowledged the need to do so; however, other priorities at

[52] Public hearing, 18.09.13, page 24

present precluded reviewing the document. She said: '*we are in the middle of a huge review of data protection legislation in Europe which will impact Jersey. My priority at the minute is establishing how that is going to affect Jersey, because it is significant. It is probably the most significant thing to happen in the field of data protection in many a year, if not since its birth. …. For anyone that follows the interest that the Commission have in data protection, it largely centres around what they call the right to be forgotten, which is trying to address, especially the younger generations, the digital trail that they leave*.[53]

220 **Recommendation**: The Panel recognises the various pressures on the Data Protection Office. Nevertheless, a review and updating of the current Code of Practice should be regarded as a priority.

Domestic CCTV issues

221 The proliferation of CCTV in private residential properties appears to be of some concern. Home security systems are relatively easy and cheap to install. CCTV cameras are being erected in increasing numbers in private residential properties, for security purposes, possibly driven by requirements from insurance companies but also by the easy availability and relative cheapness of such cameras.

222 The Data Protection Commissioner told us that her office had received a significant number of enquiries within the last year relating to the potential invasion of privacy from CCTV security cameras installed in neighbouring properties with a potential overlooking into properties. Neighbours found the presence of cameras intimidating, particularly where they might overlook their children playing in the garden. These instances were anecdotal and difficult to quantify: there were no statistics available to judge the extent of this problem. [54]

[53] Public hearing 26.06.13, page 16 - 17
[54] Public hearing 26.06.13 page 19

223 In the UK Andrew Rennison, the Surveillance Camera Commissioner, has acknowledged that government may have to address this growing problem. He has promised to publish guidance on the matter 'in the next year or so'. '*What concerns me,*' he said, '*is the upset it can cause other people. I expect to receive complaints from people about inappropriate use of CCTV, but I suspect the highest number of complaints I receive will be from private users or people who have neighbours using private systems*.'[55] This could include new laws and regulations, or could simply be a guide to the rules that are already in place.

224 However, the Data Protection Law does not apply to individuals holding information for domestic use and there is no requirement for CCTV within domestic premises to be registered with the Data Protection Commissioner[56]. There is no requirement to keep records of recordings or place signage around domestic premises where CCTV is being used unless it is for business purposes.[57]

225 The recording of images overlooking a neighbour's garden, however, does potentially have a very real impact on the people being watched. Nevertheless, there is little the Data Protection Office can do to intervene in such cases, apart from give advice to homeowners. There are basically two options:

- address the problems directly with their neighbours or
- seek the assistance of the police who might be able to treat the problem as harassment.

226 An alternative route would be to try to show that the neighbour's actions were contrary to Article 8 of the Human Rights Convention, namely the right to respect for private and family life. However, this option was likely to be difficult and disproportionate. The Human Rights (Jersey) Law 2000 provides judicial remedies only in relation to acts by a public authority.[58]

[55] http://www.telegraph.co.uk/news/uknews/law-and-order/10109384/CCTV-new-controls-on-private-security-cameras-to-stop-homeowners-snooping-on-neighbours.html
[56] Public hearing 26.06.13, page 3, 19, 41 - 44
[57] http://www.homecctvdirect.co.uk/home-cctv-uk-law.html
[58] Human Rights (Jersey) Law 2000, articles 8-9

227 The Commissioner told us that Data Protection legislation was not designed to extend to the domestic sphere: data held at home does not generally have any adverse impact in terms of privacy. Extending the law to interfere with the domestic sphere of people's lives would add a great deal of bureaucracy to everyone who used a camera and would be difficult to justify.[59] She commented: '*This is a complex problem in that it raises questions of how far the 'state' wants to interfere with the private lives of individuals. It is an interesting set of competing rights at play – on the one hand you have an individual who claims to want to be able to protect his/her property and that is his/her right. On the other, a neighbour is claiming that their rights are being infringed because of inappropriate surveillance of their home and family*.'[60]

228 The States of Jersey Police said that they did receive some complaints of this nature but they were few in number. As there was no specific legislation to cover such matters it was difficult for the police to resolve. In the majority of instances no offences had been committed and the police have no specific powers to stop it occurring. The Police added: *It is notable that the persons who are conducting the CCTV monitoring often feel that they have a legitimate reason or perceive themselves as being victims or being targeted by others. Dependent on the allegation, frequency, action and intention of those conducting the CCTV there might be a potential to consider some offences (conduct likely to cause a breach of the peace or harassment) however these would only be extreme instances accompanied by additional factors*. [61]

229 We considered whether the issue might be addressed under the Statutory Nuisance Jersey Law 1999. We spoke to the Acting Head of Environmental Health who said that his office had received no complaints of this nature. He explained that a statutory nuisance was 'something that unreasonably interferes with your enjoyment of your house or land that occurs more than once'. He acknowledged that overlooking by CCTV might conceivably affect enjoyment of one's property: for example not being comfortable with allowing their children to use a paddling pool in the garden. However, statutory nuisances were linked to injuries to health caused for example by regular noise

[59] Public hearing 26.06.13 page 45
[60] Written submission: Data Protection commissioner
[61] Briefing note for public hearing 26.06.13

disturbance: it would be difficult to prove that the psychological impact of intimidation through CCTV was a nuisance under the normal meaning of the law. Providing proof of what the system was pointing at, how long it was focussed on external areas and what is what recording would require gaining access to the system to check.

230 We also explored the potential for CCTV to be included within the planning process for domestic properties. We were mindful that policy provisions already allowed for the Planning department to prevent developments (for examples, extensions, conservatories) where potential overlooking of neighbouring properties would be created. Currently, however, the installation of CCTV is exempt from planning permission (Planning and Building (General Development) Order 2011). In Schedule 1 part 3 Class D, CCTV cameras are included in a class of works for the maintenance of a private way including lamp standards, seats, fire alarms and others.

231 The Director, Development Control, told the Panel that it was not clear whether the installation of a CCTV camera in itself could be classed as a development[62]. While the erection of a pole with a CCTV camera might be considered a development under current legislation, for the most part, CCTV cameras on domestic properties were small units attached to walls and could even be situated within a room inside a property. He said that Planning could not deal with installations on this scale; it would be necessary, if CCTV cameras were to be regulated, to define the threshold for when it would be appropriate to control cameras.

232 The Director, Development Control, said that Building Control enforcement officers would face an inherent difficulty in dealing with CCTV as the potential for overlooking could easily be altered by remotely panning and tilting the cameras. Furthermore, dome encased cameras hide the orientation of cameras.

233 We accept that Planning cannot deal with other areas of concern for example the misuse of recorded images on social media or the use of CCTV images for voyeuristic purposes, harassment, anti-social behaviour or other matters which should be dealt with under criminal law and are matters for the police to investigate.

[62] Public hearing 28.06.13, page 18

234 We note, however, that the UK does have a measure of planning control over the placement of CCTV cameras on the outside of buildings (Town and Country Planning (General Permitted Development) Order 1995). Part 33, Section A classes any CCTV camera as being "Permitted Development" unless they are in breach of a number of conditions relating to their size, location on the building and number of cameras. The Scottish version of this order contains a useful addition: *"The field of vision of a camera should, so far as practicable, not extend beyond the boundaries of the land where it is sited or any adjoining land to which the public have access. Intrusion and inconvenience to neighbours should be limited so far as is practicable without compromising the cameras effectiveness for security purposes"*.

235 **Key Finding**: The Panel acknowledges that the complexity of finding a solution to the issue of household cameras overlooking neighbouring properties but believes the Scottish development order cited above might feasibly offer a partial solution to the problem by means of regulating the installation of visually prominent cameras where there is a potential for overlooking into a neighbouring property.

- In this case the person installing the camera would require planning permission and have to demonstrate that appropriate measures had been taken to prevent overlooking (eg restricted orientation of cameras or privacy masking).
- Owners could be required to specify the location of cameras and the range of image capture.
- Systems which surveyed neighbouring properties could be rejected.
- The installer would have to erect a notice indicating his intention of doing so; this would enable the neighbours to have the opportunity of challenging the installation.
- Planning Officers could also question the purpose of having cameras sited where overlooking was possible when considering the application
- Enforcement Officers could deal with situations where cameras with overlooking potential had been erected without planning permission
- The law could be applied retrospectively to existing camera installations

236 **Recommendation**: The Panel recommends that the Planning Minister gives serious consideration to reviewing the classification of CCTV as permitted development and follows the example of Scottish legislation on this matter.

237 **Key Finding**: The Panel also believes that it would be helpful to neighbours if all domestic CCTV operators were obliged to register their systems with Data Protection. We acknowledge that this obligation is currently extra-statutory but we request the Data Protection Commissioner to consider and explain the implications of this suggestion.

Guidance

238 We have also noted that some Councils give clear guidance on the use of domestic CCTV. Mid Devon District Council, for example, contains the following statement:

> *You must respect your neighbour's right to privacy; CCTV should not be directed into someone else's home or property. As a domestic user of CCTV you are exempt from the Data Protection Act however if you misuse your CCTV system you could still face criminal or civil consequences. Using CCTV to invade another person's privacy on more than one occasion could be harassment which is a serious criminal / civil offence. Using CCTV images for voyeuristic or anti-social purposes are also offences that the police can deal with under criminal law.*
>
> *Directing your CCTV cameras onto another person's property may have serious legal consequences.*
>
> *If you intend to install CCTV it is always a good idea to discuss this with your neighbours. Should your neighbours have concerns, letting them see the images the cameras are taking may help put their mind at rest.*[63]

239 **Key Finding**: The Data Protection Commissioner has already published an extensive series of guidance notes on Data Protection issues. We believe that a plainly worded guidance note would be useful for anyone wanting to install a CCTV system at home for security purposes. This would provide an explicit warning about the potential

[63] http://www.middevon.gov.uk/CHttpHandler.ashx?id=16634&p=0

criminal or civil consequences of misusing CCTV to invade another person's privacy and might lead to a reduction in complaints. It could also usefully include guidance on the legal requirements and advice on how to use the CCTV images in the event an incident occurs.

240 **Recommendation**: The Data Protection Commissioner should prepare a comprehensive guidance note for those wanting to install a CCTV system at home for security purposes or to tackle anti-social behaviour.

The rights of access to information and camera footage by citizens

241 Requests for disclosure of images captured by public sector CCTV are rare, with the exception of the police investigating incidents. Some examples of requests for access to CCTV footage:

- Transport and Technical Services reported that they receive a small number of requests from insurance companies relating to insurance claims for vehicle damage but these are usually too long after the event to have any footage available. All requests are referred to the police.
- Requests to view CCTV footage of Millennium Park are received from staff trying to identify people who have allowed their dogs to foul an area or people who have dropped large quantities of litter. Images are only released to support prosecution in the event of a breach of Park Regulations.
- Requests are sometimes received by the States of Jersey Police to disclose images captured on the Town Centre system for civil cases such as road traffic collisions or civil disputes. In such cases CCTV images are only released with a court order or with the authority of the Director of Criminal Justice, taking into account the provisions of the Data Protection Law.

242 An individual is entitled under the Data Protection Law to see or be informed about any data, including CCTV images, held about them. The Data Protection Commissioner's Code of Practice sets out how an individual can make such a request. In summary:

- Individuals will have to specify dates and times of images they request.

- They should be provided with a standard subject access request form and a leaflet describing the types of images which are recorded and retained, the purposes for which those images are recorded and retained and information about the disclosure policy in relation to those images.
- The operator is entitled to charge a fee (maximum £10) for carrying out the search for images.64

243 A particular problem arises from the nature of CCTV images in that other individuals may also be included on the images. If providing images would involve an unfair intrusion into the privacy of a third party then it will be necessary to obscure them before release.

244 An individual's subject access rights are restricted if the images are held for the purposes of prevention or detection of crime or the apprehension or prosecution of offenders.[65] Where public space CCTV records people walking down the street, going about their lawful business and where nothing untoward has occurred this may not be necessary. However, in situations where individuals have a high expectation of privacy and confidentiality, such as in waiting room for a doctor's surgery, images of third parties should be blurred.[66]

245 Images should only be released for reasons which fall within the purposes and objectives of the scheme and should not be used for any other purpose.

246 **Key Finding:** Individuals whose images are recorded have a right to view those images and to be provided with a copy of the images. Operators' codes of practice should detail how members of the public make access requests. In practice, such requests by individuals are not common and this right is not widely known. Individuals face obstacles as it may be necessary to block out images of third parties and may be required to provide heavy justification for their request. We believe that the introduction of Freedom of Information legislation in Jersey may lead to an increase in requests from members of the public for CCTV images of themselves held by States organisations.

[64] Jersey Code of Practice and Guidance on the use of CCTV, 2005
[65] Ibid
[66] Information Commissioner's Code of Practice 2008, chapter 9

Employees' rights in relation to camera surveillance by employers

247 Employers may use CCTV quite legally to monitor their staff for a number of reasons:

- To safeguard their employees or members of the public (eg for health and safety reasons)
- To protect business interests (eg to prevent shoplifting or pilfering from stock or to deter misconduct)
- To ensure quality of customer services (CCTV can show training needs for employees)
- To comply with legal and regulatory obligations (eg airport security)

248 Under data protection legislation, CCTV monitoring must normally be open and there should be good reason for the employer to use it. An employer should carry out an impact assessment before implementing a CCTV system. They should inform their staff about the nature and extent of the monitoring. This should include notices and a written policy statement making clear how the CCTV images will be used by the employer, how they will be stored and processed.[67]

249 Covert or targeted monitoring is only justified where there are grounds to suspect criminal activity or serious malpractice by the employee in question and the monitoring is necessary to prevent or detect this crime or malpractice. This monitoring would usually then lead to a disciplinary hearing where the employer believes the employee has breached company policies. Employers are encouraged to seek advice from the States of Jersey Police before implementing covert surveillance of staff.[68]

250 In most cases, CCTV monitoring in the workplace is regarded as reasonable by staff. Supermarkets, retail stores and bars in Jersey, for example, regularly monitor their staff transactions at tills without complaint from employees. CCTV is also used in

[67] http://www.yourrights.org.uk/faqs/workplace-faqs/my-employer-is-using-cctv-to-monitor-me-at-work-is-this-legal.html ; http://www.adviceguide.org.uk/england/work_e/work_rights_at_work_e/monitoring_at_work.htm

[68] http://www.freelanceadvisor.co.uk/go-freelance-guide/workplace-surveillance-can-your-employer-spy-on-you-at-work

warehouses to monitor stock and in open areas to monitor vehicle movements. It may also be used to monitor staff clocking in to work. We have received no evidence that CCTV is used in office environments in Jersey to monitor staff performance.

251 The Channel Islands Co-operative Society told us that their staff were positive towards the presence of cameras; the purpose behind the cameras was discussed in induction programmes and there was clear signage in staff areas. CCTV was not used to monitor attendance.

252 Some employees, however, may feel that CCTV monitoring is excessive or disproportionate. Examples of this may be where cameras are put in areas where staff have a reasonable expectation of privacy, such as toilets or changing rooms. Both the Data Protection office and the Jersey Advisory and Conciliation Service (JACS) receive enquiries from employees about the legal framework that sits around the use of CCTV at work.

253 Staff may also feel that continuous monitoring is overbearing. An example of this in Jersey was a complaint by drivers in Liberty buses which have fitted cameras monitoring passengers entering their buses and transacting with the drivers. A number of buses also have audio recording above the driver's head. The drivers felt that they were under constant surveillance and that their conduct was being targeted by the management. They were also aggrieved about the dismissal of a driver where CCTV footage had been used in evidence in a disciplinary case. The example shows how CCTV can engender or exacerbate a lack of trust between management and workforce.

254 JACS advised the management at Liberty Bus to ensure that the drivers understood the rationale for the cameras and the scope of legitimate use. The Panel raised this issue with the General Manager, who said that concerns by drivers had been allayed once the purposes of the cameras had been clarified. Buses were monitored in this way to protect its passengers and its staff from assault or other abuse as well as protecting the employer's property, including cash. Images were only monitored when a specific complaint or incident was under investigation. Unite the Union confirmed that drivers now had a better understanding of the policy but remained cautious.

255 JACS said that they were aware of CCTV recordings being used regularly in providing evidence as part of investigations into alleged disciplinary offences (a dozen or more instances of this each year). JACS commented: 'It is not unusual that the request for CCTV footage to be viewed originates from the staff member who is being investigated (to provide evidence that he/she did not act improperly) as well as by the employer. In other words CCTV footage has been used to the benefit of employees as well as employers. We have not heard of instances where an employer has unreasonably refused to allow an employee access to CCTV footage when access may be pertinent to that employee'.[69]

256 JACS told us that they had no reason to be concerned that the overt use of CCTV was regarded as unreasonable by the large majority of employees.[70]

257 Unite the Union informed us that they dealt with an increasing number of enquiries from members who were nervous about aggressive use of CCTV by employers who appeared to be unaware of data protection principles. They felt that ignorance on the part of employers was an issue. Problems occurred when staff were not properly informed about the use that might be made of footage; or when managers appeared to put up cameras at a whim. The Regional Officer, Unite, said employers were tempted sometimes to extend the original stated purpose for CCTV. He cited two examples of companies using CCTV, established for security purposes, as a means of monitoring taking unauthorised breaks and as evidence in disciplinary cases, without informing staff about extending the purpose of CCTV. He said that few companies had adequate policies or codes of practice relating to procedures, retention policies and security of CCTV. He advised his members to refer to their staff handbook or contract and to notify management where they believed that there were breaches in compliance.[71]

258 **Key Finding**: There are legitimate uses of CCTV in the workplace; for example in monitoring till transactions in bars and supermarket or movements of stock in warehouses. We have received no evidence that CCTV is used in office environments in Jersey to monitor staff performance. Where employers make staff aware of the purposes

[69] Written submission: JACS
[70] ibid
[71] Meeting dated 26.09.13

and scope of this surveillance and make clear policies available on procedures for the security, processing and retention of images employees generally find no reason for concern about the overt use of CCTV. However, employees find that continuous monitoring, where this occurs, is overbearing. Complaints occur when employers use CCTV for monitoring purposes outside their stated policies and procedures.

12 Conclusion: Developing the formal regulation of the use of camera surveillance in Jersey

259 There is currently limited formal regulation governing the use of CCTV in Jersey. In the UK the government has brought forward new proposals to drive up standards and regulate further this important area. Our review has identified areas where the provision and governance of CCTV in Jersey can be improved, in particular:

Data Protection Code of Practice and Guidance on the Use of CCTV

260 The Data Protection Commissioner has published a Code of Practice which applies to the use of cameras in public spaces together with guidance to businesses on the standards which must be followed to ensure compliance with the Data Protection (Jersey) Law 2005.

261 It is apparent that some aspects of this Code should be reviewed to ensure that it is brought in line with best practice elsewhere in Europe. The Code should incorporate the following (these are standard practice elsewhere):

- A requirement for signage, including contact details for the operator
- A log of visitors to the CCTV control room
- A log of all (including informal) access to CCTV footage
- A standard retention period for public services
- A periodic review of effectiveness and costs of cameras and systems
- A requirement to specify where data matching takes place
- Live targeting: There should be a requirement for appropriate training and audit of targeted surveillance and a statement on the acceptable length of time for following a suspect without any concrete grounds for reasonable suspicion

262 The Data Protection Code of Practice requires updating to ensure that it is brought in line with current developments.

Public engagement and awareness

263 The notion of 'surveillance by consent' which is central to the recently published Home Office Surveillance Camera Code of Practice, requires the public to be informed about the purpose(s) of public space CCTV and the location of cameras, as well as consulted about new cameras or the expansion of existing systems.

264 Currently the main town centre system in St Helier does not have any public signage. The public do not know therefore that the system is a 'police' system used for operational issues, or who to contact in relation to the operation of the system and the processing of personal data.

265 The requirement for public engagement could be embedded in the Code of Practice. This should be an important element in the States of Jersey Police project to renew and extend the current Town Centre CCTV system. The Police should publish a map showing the location of all public space cameras in their system.

Register of cameras

266 The Code of Practice requires every 'data controller' to register annually the existence of a CCTV system with the Data Protection Commissioner. Operators should also have their own code of practice setting out the purpose of their systems and policies on their operation. (Note: this requirement does not extend to homeowners who have installed CCTV for their own domestic security).

267 This statutory requirement provides little knowledge about the number of cameras, their capabilities, how these are upgraded or the compliance of the operator with the Code of Practice. It would be relatively easy and inexpensive to supplement this process in order to keep a record of the existence of cameras and other aspects of their use.

268 We suggest that the statutory annual returns should be supplemented with an additional information request, preferably one sheet of paper, capturing information such as the number of cameras in a system, their location, the existence of a Code of Practice, primary and secondary purposes, links to other databases and aspects of their technical capability.

269 An annual review of the number and types of CCTV could be presented to the Minister for Home Affairs by the Data Protection Commissioner (based on the CCTV register). This would allow some political debate and oversight.

270 A register of CCTV systems in the Island should be compiled by the Data Protection Commissioner and made publicly available.

Evaluation Mechanisms

271 The Code of Practice includes advice for CCTV operators to undertake an internal annual assessment which evaluates the effectiveness of the system against the stated purpose of the scheme. The Code states that if the scheme is not achieving its purpose it should be discontinued or modified. The Code also includes advice on maintaining the quality of images in order to ensure that images are effective for the purposes(s) for which they were intended.[72]

272 There should be a requirement that public sector CCTV operators undertake a minimum standard of evaluation annually to ensure that their systems are effective, appropriately sited and are achieving the purpose set for them. Systems which do fulfil their security purposes should be removed.

Domestic CCTV

273 There appears to be increasing concern about the use of CCTV on residential properties impinging on the privacy of neighbours. This is a complex issue as data protection legislation does not cover the use of CCTV in the home.

274 We suggest that the Planning process offers a means of regulating the installation of cameras with a potential for overlooking. Owners could be required to specify the location of cameras and the range of image capture. Systems which surveyed neighbouring properties could be rejected.

[72] Code of Practice, pages 18 and 10

275 In addition, the Data Protection Commissioner should issue guidance for home owners who wish to install CCTV systems as an aid to security or to tackle anti-social behaviour.

Appendix One: External Advisers' Final Report

States of Jersey Education and Home Affairs Scrutiny Panel

Review of Camera Surveillance

Professor Peter Fussey, University of Essex

Professor William Webster, University of Stirling

December 2013

Professor Peter Fussey

Department of Sociology

University of Essex

Wivenhoe Park

Colchester

Essex

CO4 3SQ

Tel: 01206 872748

Email: pfussey@essex.ac.uk

Professor William Webster

Centre for Research into Information, Surveillance and Privacy (CRISP)

Stirling Management School

University of Stirling

Stirling

FK9 4LA

Scotland, UK

Tel: 01786 467359

Email: william.webster@stir.ac.uk

CONTENTS **Page 85**

SECTION ONE: Introduction

1.1 Introduction

This document represents the External Advisers' Final Report for the States of Jersey (SoJ) Education and Home Affairs Scrutiny Panel Review of Camera Surveillance. The report has been prepared by the External Advisors: Professor Peter Fussey, University of Essex and Professor William Webster, University of Stirling. The Scrutiny Panel's Review of Camera Surveillance took place from April to December 2013 and considered the use of video surveillance cameras, also known as CCTV (Closed Circuit Television), in a range of public and private settings in Jersey. The review incorporated evidence from a number of sources, including: Scrutiny Panel Hearings (public and private sessions), an online public survey, site visits, correspondence and written submissions. The External Advisors have supported this process and have produced an 'Initial Impressions Report' and a 'Preliminary Findings Report', both of which have fed directly into this published 'Final Report'.

The report consists of three main sections. Following the introductory section (Section One), the report sets out the main findings of the Review (Section Two). This is followed by a section covering conclusions and recommendations (Section Three).

1.2 Terms of Reference

The Terms of Reference for the States of Jersey Education and Home Affairs Scrutiny Panel Review of Camera Surveillance are attached at Appendix 1. Broadly, the review was designed to consider:

- The prevalence of camera surveillance in Jersey,
- The effectiveness and impacts of camera surveillance in Jersey,
- Public attitudes towards camera surveillance in Jersey, and
- The appropriateness of camera governance/regulation arrangements in Jersey

This is a wide-ranging remit which covers a range of camera systems in a number of different locations. It encompasses camera surveillance in public places, in private settings and in domestic dwellings. It captures a range of different systems, including the St Helier town centre system, and systems in shops, hotels, schools and car parks. Technical capability and operating practices also differ from system to system. It is important to note from the outset that the review did not consider camera surveillance established for covert investigations or the use of other surveillance technologies.

1.3 Overview of Findings

Although the review of camera surveillance in Jersey was wide ranging there are a small number of key findings:

- There are a number of CCTV camera surveillance systems operating in public places[73] on the Island of Jersey. Most of these systems are relatively small, in terms of camera numbers, but combined they represent a significant deployment of surveillance technology.
- Existing systems differ in purpose, technological capability and operational practice.
- Among operators there is an increased interest in newer forms of CCTV, such as body-worn cameras and ANPR, along with a proliferation of cameras into new locations such as public and private transportation and domestic settings.
- There is an overwhelming view among operators that CCTV provides a vital function in enhancing public safety and reducing crime and disorder in Jersey.
- There is some evidence of public support for CCTV in Jersey.
- Because of the small population, there is a high likelihood that CCTV operators will recognise subjects (the surveyed) throughout any given shift. The governance of

[73] Public' and 'public place' are defined in accordance with the 2013 UK Surveillance Camera Code of Practice. This definition is drawn from Section 16(b) of the Public Order Act 1986 and includes any highway and place which the public or any section of the public has access (by payment or otherwise) as of right or by virtue of stated or implied permission. Thus public spaces and public space camera systems apply to spaces where the public have regular access to and may include areas that may be privately owned.

surveillance practices is therefore critical to retaining confidence in the appropriate use of systems.

- The Data Protection Commissioner has issued a Code of Practice (CoP) to govern the use of CCTV in public places. This is now out dated and should be brought in line with best practice elsewhere in Europe. Despite claims to the contrary, there is little evidence of compliance with the CoP or that compliance with the CoP is being monitored. For example, it is evident that not all CCTV operators had a CCTV CoP.

- The current operation of CCTV by the SoJ Police falls short of what is seen elsewhere in the UK and Europe, both in terms of 'day to day' operation and the governance of systems. Consequently, it is difficult to be confident that the police use of CCTV is appropriate, justified or fair - this is not to say that systems are misused by the SoJ Police. Appropriate governance arrangements, performance assessment mechanisms, an updated Police Code of Practice, and the introduction of auditable processes should be introduced as a matter of urgency to ensure the delivery of a service in the public interest and to ensure compliance with UK and European standards and norms in the provision of CCTV. Updated practices are likely to result in greater public confidence in the Police use of CCTV. This is vitally important for the ongoing SoJ Police provision of CCTV in Jersey and should be a necessary requirement before the Police systems are expanded or digitised.

SECTION TWO: Camera Surveillance in Jersey

The findings presented in the Externals Advisor's Final Report are organised around 13 core topics.

2.1 Consultation and Consent

'Surveillance by consent' is becoming a key element of CCTV practice in the UK and EU, especially in relation to the provision of public space systems in town and city centres. We have not encountered any initiatives that seek to understand the extent to which surveillance operates on a consensual basis in Jersey. Statements such as 'everyone recognizes the benefits' of CCTV are often expressed, and may be true, but no evidence has been offered to support such sentiment. There is no evidence of those operating public space surveillance cameras engaging in any meaningful public or service user consultation.

Public surveillance needs to be conducted on the basis of consent. Consent needs to be evidenced rather than simply assumed. Good practice would be for a robust public and/or service user consultation, based on minimum principles of objective research, to be conducted prior to the installation of cameras in public spaces. If organisations responsible for operating the cameras feel there is insufficient expertise to conduct a wide-ranging and objective consultation then the cost of commissioning this activity should be considered part of the capital funding associated with the overall installation of the system. In most of the UK, local authorities operate large public space CCTV systems and public consultation is a normal part of the process of installing cameras and systems. The situation in Jersey is slightly different in that the SoJ Police operate and maintain the large public space system in St Helier. It is our view that this situation makes regular public consultation even more important. There is a delicate power relationship between citizens and the police and it is important that CCTV is not perceived as a police tool to 'spy' on people. Appropriate public consultation and awareness exercises are therefore critical in ensuring continued public support for the SoJ Police operation of CCTV.

If levels of public support are ambiguous and inconclusive, alternative crime prevention/order maintenance strategies should be deployed. Moreover, if 'smart' CCTV analytic capability is to be added to existing cameras, then similar consultation should be carried out to ensure that consent exists to legitimate such activities. If public approval were proven to be as high as many practitioners imagine, then such evidence would also give them a robust mandate for their activities. We would expect public engagement to be an element of the SoJ Police

CCTV Code of Practice. Other operators using CCTV in public places should, following current best practice, consult with citizens and their service users about the deployment of CCTV. This is the case for public services and for private operators using CCTV in public places.

2.2 Monitoring Performance and Effectiveness

Few, if any, formal mechanisms to monitor the long-term effectiveness of cameras exist in most of the systems we reviewed. During one public hearing the SoJ Police representative argued that it would be 'too expensive' to monitor the effectiveness of cameras. In other domains, notably the use of surveillance cameras in some education environments, once budgets have been devolved to their discretionary holders we encountered little reflection on how surveillance cameras are operated or any analysis of their efficacy.

We accept that evaluation processes may be complex and onerous but, equally, some simple measures could be introduced to improve this situation. We also consider it possible to argue that a straightforward evaluation of system effectiveness could prove less expensive than new inappropriately or ineffectively sited camera installations. Moreover, if understanding of the uses and applications of CCTV were limited, then it would follow that knowledge over the extent to which systems are used properly and effectively is also restricted. If the cameras are not proven to be offering security then, arguably, incursions into privacy become less justifiable. Given this lack of analysis, the SoJ Police controlled CCTV system, along with those administered by other organisations, do not meet the requirements for monitoring effectiveness laid out in Jersey's Data Protection Commissioner's CCTV Code of Practice and cannot be said to be fully compliant in this regard.

To address this shortcoming, we recommend that formal monitoring of the effectiveness of public surveillance camera systems be undertaken on at least an annual basis. All CCTV operators should identify a set of simple performance indicators that are auditable and reported on periodically. The indicators could include: detail on surveillance events (such as the number and types of offence captured), number of requests to review footage and whether footage was used in the prosecution. Indicators could also include a range of administrative information, such as: number of operators and shift patterns, training completed, periods when cameras are inoperative, number of occasions when excessive surveillance took place (where surveillance is concentrated on an individual for more than

the agreed number of minutes), a log of public enquires, and occasions when the CCTV Data Controller/Manager reviewed surveillance practices, etc. We would also recommend including some comparison of the crime rates in areas observed by CCTV against those without coverage in order to assist understandings of crime displacement and to provide and evidence base to inform future camera deployment decisions. This process should be followed by a review of the appropriateness of existing camera positioning. We believe that appropriate performance measurement will ensure the best deployment of systems and secure public confidence in the way systems are used. We would also like to point out that where camera systems are provided by public services there should be an onus to demonstrate value for money and to be accountable to political processes. Both can be achieved more easily with appropriate performance indicators and audit procedures.

2.3 Proportionality

The Panel were regularly informed that Jersey's public surveillance camera systems constituted a 'proportionate' response to various crime, disorder and anti-social behaviour issues. However, it was less clear how calculations of proportionality were determined and in some cases it was not clear why surveillance cameras were deemed a proportionate long-term response to these issues. Current best practice in the UK and Europe, evidenced by the UK Surveillance Camera Commissioner's CoP and the forthcoming European Data Protection Directive, points to a requirement to clearly specify the purpose of systems, to justify their proportionality (and the need for surveillance) and to measure the performance of systems against agreed purposes. This requirement is designed to ensure that the mass collection of personal data is for a legitimate purpose, that proportionality can be demonstrated, and to ensure that 'surveillance creep' (where a system introduced for one purpose is then used for another) does not take place.

Surveillance via CCTV must have a clearly defined purpose and activity must be measured and audited (see above). Moreover, less intrusive alternative measures should be considered and only discounted if deemed inadequate for achieving these ends. Linked to the aforementioned theme of surveillance by consent, another element of a proportionality test could involve consideration of the competing interests of different groups likely to be affected by new surveillance practices. Alternatively, establishing proportionality could be achieved by comparing surveillance infrastructure and practices in Jersey with those in the UK and other parts of the EU. For example, many surveillance camera footage retention

periods in Jersey far exceed those in the UK despite there being no evidence of higher levels of offending.

Many contributors to the Panel highlighted the significant order-based problems associated with St Helier's night-time economy. We would expect it would be easy to make a case that surveillance cameras are a proportionate response to the quite evident problems here. However, we would contend that it is much more difficult to argue an ANPR system logging details of every vehicle travelling on all arterial roads in and out of St Helier is proportionate. A similar system in an English market town has recently been designated as illegal by the UK Information Commissioners Office. Part of any proportionality test, and of appropriate use of surveillance technologies more generally, should be a clear definition of specific purpose of the system. This is a legal requirement under Data Protection legislation.

2.4 Disclosure, Accessing Surveillance Camera Footage and Entering Operation Rooms

There appears to be no register of access to any of the CCTV suites we observed. This is standard practice elsewhere in Europe. Whilst variations of practice do exist, a requirement to sign in, provide identification and a reason for visiting is normal procedure in most CCTV control rooms across the EU. We encountered no similar practices in Jersey. We strongly recommend that access to any surveillance camera suite, or similar facility where monitors are located, is logged. This log should include details such as the name of the visitor, time of visit, purpose and name an employee responsible for escorting the visitor.

A related issue concerns informal access to, and requisitioning of, images and personal data. It is apparent that informal and potentially improper review and requisition of surveillance footage has taken place on occasion. Whilst we accept that, for operational purposes, expediency is sometimes required during the act of requisitioning data, safeguards should be put in place to minimise any improper requests. We recommend all requests to review surveillance camera footage, by anyone, be subject to a formal procedure involving the logging of names, reason and times of request. This is a necessary requirement to be compliant with Data Protection legislation. We would anticipate a streamlined auditing process to give data handlers the best chance of compliance. Such activity is essential if the general public are to be confident that systems are operated according to best practice.

2.5 St Helier Public Space System Upgrade and Expansion

The SoJ Police are currently in the process of extending and updating the St Helier public space CCTV system. However, further clarification is required concerning the evidence used to inform decisions over camera deployment and network expansion. The scrutiny process revealed that among those considering the expansion of Jersey's public surveillance camera network place a high value on tacit and experiential judgment. These are appropriate forms of information, although we would expect such information to be supplemented by more objective measures, such as offence mapping and public engagement. In this respect, the 'need' for every camera should be established and periodically reviewed. Furthermore, the 'need' for individual cameras should be backed up with public consultation and direct engagement with those living in residential properties surveyed by such cameras.

The proposed upgrade to the St Helier's public space system would make it fully digital. Although new cameras are not proposed at the moment, once the system is digitised it would be relatively easy to add further cameras to the system. Furthermore, a digitised system will make it much easier to add in camera analytics, such as face, movement or object recognition software (although we note that the SoP Police report no plans to do this at the moment). In this respect, the move to a digital system is a very significant development as it opens up the possibility of far more intrusive surveillance practices than are currently possible. Given the current lack of safeguards, the obsolete SoJ Police CoP and the lack of public consultation (all discussed in more detail elsewhere in the Report), it is our considered view that such a network upgrade is inappropriate until such time that the SoJ Police adopt appropriate governance arrangements for their provision of CCTV.

Elsewhere in the UK, most local authorities undertake public consultation to identify local perceptions of crime and disorder and to gauge general levels of acceptability. Moreover, there has long been recognition that surveillance cameras work poorly when operated in isolation. Consequently, to represent an appropriate use of public resources CCTV cameras are usually installed in combination with other crime reduction strategies. We recommend that good practice in this area would involve the use of multiple objective forms of evidence to inform decisions over the installation and location of new surveillance cameras. Sources of information should include measures of crime and disorder rates; description of crime type; deliberation that surveillance cameras are the correct, effective and most appropriate tool to address these incidents and; a measure of acceptability by users and residents of the proposed site for deployment.

2.6 Signage

Signs are a way of making people are aware that they are under surveillance and are therefore an essential way of ensuring surveillance by consent. The main town centre CCTV system in St Helier does not incorporate any signage about informing citizens about the existence and purpose of the cameras. Signage is now standard practice elsewhere in Europe. When asked, the police and other participants in the Review have not identified any way that signage would impede operational practices.

In our view, some the most helpful guidance on surveillance camera signage can be found in the UK Information Commissioner's Office *CCTV Code of Practice* (ICO 2008). This guidance asks that signs should be placed in prominent positions at the entrance to a location covered by CCTV. Signs should also be more prominent and frequent in places where cameras placements are less obvious or people would not expect to be under surveillance. For public space CCTV, signs should convey key pieces of information including the purpose of the cameras, the organisation monitoring them and contact details for those administering the cameras. Whilst there is some mention of signage in the existing Data Protection Commissioners CCTV CoP, it could be more developed to include some of the details outlined above.

Among the very mixed research evidence relating to CCTV effectiveness, one of the few areas of consensus relates to its value as a deterrent against high volume crime (Welsh and Farrington 2002; Fussey 2008). In addition to facilitating greater degrees of surveillance by consent, prominent signs advertising the existence of cameras are thus likely to assist their deterrence-based crime reduction benefits.

2.7 Census of Surveillance Cameras

A register or census of cameras and their purposes is currently absent. Creating one could make it easier to ensure compliance to regulations and codes of practice and place Jersey at the forefront of European best practice in this area. This could be achieved though a short extension to the data controller's annual submission form to the Office of the Data Protection Commissioner. Data controllers could be asked to state the number of cameras they operate, their location and purpose. This could be achieved with minimal effort and cost. The Data Protection Commissioner's Office would then hold a continually updated central register of cameras on the island. In a further extension of this good practice, non-covert camera locations could also be made publically available, for example, via the Data Protection Commissioner's Office or SoJ Police website. This could also increase any deterrence

effects of the cameras. The extent of camera surveillance and key trends could then be presented to the States periodically, thereby providing opportunities for political oversight.

2.8 Private CCTV and Domestic Dwellings

Throughout the scrutiny process we were informed about particular problems concerning private individual's use of cameras in and around their homes in Jersey, particularly when private cameras in domestic dwelling captured images from neighbouring properties. Despite numerous attempts we were not able to find any evidence regarding the frequency of complaints in this area. It is also evident that current legislation governing the use of CCTV does not apply to residential properties.

With the increasing availability of low cost domestic CCTV hardware we suggest that some form of regulation in this area would be appropriate in order to shape future installation and surveillance, to provide opportunities for redress and to avoid any escalation of the problem. That said, the lack of evidence concerning the prevalence of such complaints suggests that intervention should build on existing regulatory mechanisms rather than creating new legislation and regulatory procedures.

We investigated a number of options for the regulation of domestic CCTV including revisions to existing regulatory and legislation governing data protection, nuisance behaviours and planning, as well as existing civil law instruments. From the evidence given to the Scrutiny Review it appears that the planning system is the most appropriate area from which to regulate domestic CCTV. Restrictions already exist on the installation of domestic CCTV under extant permitted development guidelines. These currently attend to cameras erected on poles unattached to any property. We suggest that these permitted development guidelines be modified to include explicit mention that pan-tilt-zoom (PTZ) enabled cameras or static cameras with a field of vision covering a substantial proportion of a neighbouring property fall outside of permitted development allowances.

The Environment and Planning Department raised concerns about the enforcement of transgressions, difficulties of monitoring compliance and queried the powers of Planning Enforcement Officers to view domestic surveillance camera footage. Whilst we recognise these concerns, the Department also stated that most reports of planning transgressions originate from the general public. We would not expect enforcement officers to enter properties to view footage but, rather, make a judgement on the direction and scope of a camera from an external visual inspection. If, via permitted development allowances, the

planning system was used to regulate domestic CCTV in this manner, it could place the onus on home owners and installers to ensure their cameras are compliant and would provide a recognized mechanism of redress for aggrieved neighbours.

Moreover, the Data Protection Commissioner's Office Code of Practice for surveillance cameras could be amended with regard to such domestic uses of CCTV. At present the Code states "the user should consult with the owners of [adjacent] spaces if images from those spaces might be recorded" (page 8). This could be strengthened to say "the user should seek approval from the owners of such spaces" and possibly drop the clause "if images from those spaces might be recorded". The Data Protection Commissioner's Office should also produce specific guidance information about the use of CCTV in domestic residential settings.

2.9 Data Retention

In Jersey personal data captured by CCTV is stored for varying lengths of time across different organisations using cameras. In almost all cases, the length of time exceeds image retention periods elsewhere in the UK and Europe. Some CCTV operators, particularly the SoJ Police, have articulated a reason for such lengthy periods. However, a case needs to be made for why the SoJ police and other operators require much longer periods of data retention (sometimes triple) than, say, London's Metropolitan Police, given the significantly lower levels of crime and disorder in Jersey.

Best practice elsewhere in the UK suggests that personal date in the form of images should be kept for around a month before deletion or becoming recorded over. As the Home Office *National CCTV Strategy* puts it, '[t]his time period allowed the police the opportunity to recover CCTV evidence and respond to lines of enquiry that were not known at the time the incident was reported' (Home Office 2007: 31). There is an acceptance that 31 days constitutes a retention period sufficient for police investigations to have commenced. The 31-day limit was also advocated by the UK Information Commissioner's Office. During our involvement with the Scrutiny Panel we did not encounter any arguments to suggest that Jersey experienced unique circumstances that would necessitate extended retention periods. We would therefore recommend that image retention periods for all operators using CCTV in public spaces are limited to 31 days. This should be specified in the Data protection Commissioner's CCTV CoP.

2.10 Data Matching

Clarification is required concerning the matching of surveillance camera images to data held on formerly distinct databases and concerning the use of new information that is created from the merger of these different information systems. For example, ANPR footage is linked to DVS data as a matter of course. Whilst data matching may be justifiable, proportionate and appropriate in many settings, data matching activities risk data being used for purposes other than that which it was first created. Such practices have a higher risk of conflicting with core principles of data protection, privacy and the consent of those asked to supply information about themselves. Data matching processes may also take place without the knowledge of those subjected to it. Such practices are not covered by the existing CCTV CoP and should be addressed as a priority. In doing so, we recommend that data handlers are obligated to adopt specific safeguards and engage in the regular monitoring of their activities to ensure these safeguards remain effective.

We recommend that these safeguards comprise a number of key principles. First is the principle of 'transparency'. Details of the matching of video images with databases should be made publically available and clearly set out in the relevant CoP. This should contain information that outlines the purposes of data matching, information requested and how it is to be used. For example, ANPR systems at public car parks should be accompanied by prominent signs that detail how images of customers' vehicles will be match to DVS records. This will allow customers to remain informed of how their data is used and provide an opportunity to opt out of the data matching activity by parking elsewhere. Data matching activities should also operate on a 'minimalist' basis. Only information that is relevant and necessary to complete a particular operation, rather than entire records, should be sought or shared. Once information is matched, it becomes a new form of data. This should be subject to the same access restriction and data retention periods as those outlined above.

2.11 Codes of Practice

There are a number of Codes of Practice (CoP) for surveillance cameras in operation in Jersey. However, it is evident that not all operators had a CCTV Code of Practice. The Data Protection Commissioner has issued a Code of Practice (2005) governing the use of cameras in public places, which, in our view, contains some sound principles but is in need of updating. Moreover, it is clear that many of the recommendations outlined in this Code are not put into practice.

Additionally, every operator of surveillance cameras located in a public space or a location to which citizens have easy access should have a publically available CoP. Because of the diverse placements, purposes and uses of cameras it is reasonable to offer the choice to surveillance data handlers to either adopt a standard CoP as recommended by the Data Protection Commissioner or develop one that applies its principles to their specific operational domain. Regardless of which choice is made, there should be a strong synergy between the principles expressed in the Data Protection Commissioner's updated Code and individual organisational-specific equivalent documents. Thus individual CCTV operator's Codes should be compliant with the Code issued by the SoJ Data Protection Commissioner.

Having reviewed the existing SoJ Data Protection Commissioner's Code and its application in various operational environments, we recommend consideration be given to updating a number of areas. This would bring it in line with best practice elsewhere in the UK and Europe. Areas where the existing Code of Practice could be improved are:

- Signage**.** The Code of Practice should develop existing content to express a requirement for operators to provide signage in publically surveyed areas. This is normal practice elsewhere. Signs should include information about the operator, the purpose of the systems and contact details.

- Surveillance by Consent. The CoP should contain a requirement concerning the need to seek consent from the surveyed, i.e. signs for public and private spaces, and a requirement to undertake public consultation exercises ahead of new camera installations.

- Public Awareness**.** The CoP should contain a requirement to make the public aware of the purpose(s) of CCTV and the location of cameras. This is especially the case for those living in dwellings in surveyed areas.

- Evaluation. The CoP should include a requirement for CCTV providers to evaluate the purpose and effectiveness of their systems. Page 10 of the existing CoP states "It is important that the images produced by the equipment are as clear as possible in order that they are effective for the purpose(s) for which they are intended". The theme of evaluation is picked up again on page 18. We recommend there should be a requirement that public CCTV operators undertake at least a minimum standard of evaluation to ensure their systems are effective and appropriately sited.

- Access to Footage/Control Rooms**.** The CoP should include a requirement to register access to control rooms and CCTV footage. Such records should be audited. Most UK CCTV control rooms restrict and log access to these areas. We have not encountered similar practices in Jersey.

- Surveillance and Live Targeting**.** We recommend the CoP should include a requirement for appropriate training and the audit of targeted surveillance practices. There should be a statement on the acceptable length of time for following a suspect without any concrete grounds for reasonable suspicion. This is considered good practice elsewhere.

- Data Matching**.** The CoP should include a requirement for data handlers to specify (to both the Data Protection Commissioner and to citizens via publically available documentation) where the matching of personal data takes place, with whom and for what purposes. In this respect, data should only be matched with named databases (i.e. ANPR images with the official vehicle licensing database) and not be matched with other unnamed databases. We recommend the introduction of a mechanism to regulate such activities.

- Register of Cameras**.** The CoP could include a register of systems/cameras. This would ensure greater transparency surrounding the proliferation and use of CCTV in Jersey and provide opportunities for political oversight.

- Public Space Definition. a revised Code of Practice could offer a definition of public space in order to clarify which surveillance camera operations are most duty-bound to adhere to its principles. We would recommend that this definition be drawn broadly. As stated above, the UK government Surveillance Camera Commissioner's Code of Practice defines public space in accordance with that articulated in Section 16(b) of the Public Order Act 1986 and includes any highway and place which the public or any section of the public has access (by payment or otherwise) as of right or by virtue of stated or implied permission. Thus public spaces and public space camera systems apply to spaces where the public have regular access to and may include areas that may be privately owned. Such a broad definition would remove ambiguities over what constitutes public space, ultimately ensure responsible and ethical uses are embedded across a range of surveillance

Beyond the SoJ Data Protection Commissioner's CCTV CoP it is essential that every operator using CCTV in public spaces adopt an appropriate CoP. From the evidence presented to the Scrutiny Panel it is apparent that some operators do not have a CoP and

others have codes that are extremely out of date. We recommend that this is an area that requires immediate attention.

2.12 Monitoring Compliance and Auditing

As noted above, the Data Protection Commissioner has issued a Code of Practice to govern the use of CCTV in public places. This is now out dated and needs to be adapted to the range of different data handlers and emerging forms of technological surveillance. We encountered many incidences of very limited compliance with the existing Code. For example, the Scrutiny Panel heard of numerous incidences where the Data Protection Commissioner's guidance on the recording of all requests for access to or for disclosure of surveillance camera footage was not followed. We also saw little evidence that the requirements covering on subject access (pages 16-17) was being adhered to by data controllers. The same may be said about the request to monitor the effectiveness of systems and many other areas of the Code. Because of this, it is essential that any new Code of Practice and regulatory initiative contain mechanisms to ensure compliance to the Code.

In sum, surveillance data handlers should adopt a newly revised Code of Practice or develop one that applies its principles to their specific operational domain. Codes should be made available to the public. Organisations should institute measures to ensure compliance with this Code of Practice. These measures should incorporate at least three core elements. First, an obligation and responsibility for monitoring compliance should be mapped onto a clearly defined individual or professional role. Second, a review of compliance should be undertaken regularly and no more infrequently than on an annual basis. Third, compliance monitoring should be accompanied by a mechanism to address any shortcomings.

2.13 Training

Surveillance camera technology is becoming more sophisticated and across the EU there has been a growing tendency to see its operation in more specialised and professionalised terms. In the UK for example, CCTV management has been increasingly described as a 'forensic' activity. Such developments underline the importance of ensuring staff are professionally trained in a number of key areas. During the scrutiny process we saw and heard of examples of exceptionally good practice yet we also encountered a degree of variance in the standards being applied in different control rooms. We recommend that

professional training of camera operators takes place on a regular basis. Recognisable professional standards do exist in this area (with the SIA training a minimum standard) but we would argue that explicit training needs to attend to ethical obligations, regulatory responsibilities, privacy, issues of data handling and protection, responsible subject monitoring and access requests.

At present there appears to be inconsistency in the ways data handlers are informed of their obligations towards data protection and privacy. In one instance a wall poster detailing a few obligations was used as a means to 'train' staff in these areas. As such, there is no mechanism to understand whether this information has been adopted by staff or embedded within practice. We recommend that in addition to the process of monitoring compliance to the code of practice (outlined above) managers, or a named individual, holds a responsibility to ensure new and existing staff are properly trained in these issues and that this follow-up training is provided on a regular basis to ensure changes in the regulatory environment are accommodated.

SECTION THREE: Conclusions and Recommendations

3.1 Conclusions

The Scrutiny Review of 'Camera Surveillance in Jersey' had a wide-ranging remit and gathered a large amount of evidence. In general, and in relation to the Panel's Terms of Reference (Appendice 1), we found:

- That there are a large number of mostly small camera surveillance systems operating in Jersey, and that these systems differed in their technological capability, operational arrangements and purpose.

- That the use surveillance cameras in Jersey is usually justified by their perceived contribution to reduced levels of crime, disorder and anti-social behaviour. Whilst this may be the case very little objective evidence is available to back up the efficacy of systems. It was also noted that CCTV has proved to be very useful in providing evidence in prosecutions and in assisting the SoJ Police in their day-to-day operations.

- That there is a degree of public support for the use of surveillance cameras in public places.

- The existing governance arrangements for the regulation of CCTV are not always complied with and do not meet best practice elsewhere in the UK and Europe.

3.2 Recommendations

A number of recommendations emanate from the Review of camera surveillance in Jersey, these are listed below:

1. Public surveillance measures should operate with the consent of the public

'Surveillance by consent' should be a guiding principle for the provision of surveillance cameras in public places. There are multiple ways to achieve this:

- Genuine and substantive consultation with citizens and service users exposed to surveillance (this is especially important when new cameras are installed, systems is expanded or if 'smart' analytical features are added to existing systems).

- Service provider should undertake activities to enhance public and service user awareness of camera surveillance. This would include the provision of information about camera locations, the purpose of systems and any data matching that may take place. Citizens living in dwellings exposed to surveillance should be contacted directly to ensure that they are aware of the relevant surveillance practices.
- All public space systems should incorporate signage in appropriate prominent positions.
- The Data protection Commissioners' CCTV Code of Practice should incorporate a legal requirement to comply with the principles of surveillance by consent, including a requirement for signage, consultation and public awareness mechanisms.

2. Public surveillance camera managers/operators should undertake a formal monitoring of the performance and effectiveness of camera systems

The evaluation or audit of the performance and effectiveness of camera systems should be undertaken periodically and not less than once a year. A series of performance indicators should be established which relate to the purpose of the camera system (as specified by the Data Controller). Evaluations should include, but are not restricted to:

- The frequency and types of offence captured.
- The number of requests to review footage (and when and by whom).
- Whether footage was used in the prosecution.
- How many times the control room was visited (and when and by whom).
- The number of times targeted surveillance took place (where individuals were followed for longer than the agreed time period).
- An analysis of crime statistics in surveyed areas.
- The results of consultation undertaken during the review period.
- Operator training completed.
- Auditable processes to demonstrate management checks on surveillance practices.
- Frequency of inoperative cameras and other equipment.

- Log of citizen requests for information.
- Auditable process to demonstrate compliance with the Data protection Commissioners CCTV Code of Practice.

We would also recommend including some comparison of the crime rates in areas observed by CCTV against those without coverage in order to assist understandings of crime displacement and to provide and evidence base to inform future camera deployment decisions. This process should be followed by a review of the appropriateness of existing camera positioning.

3. A formal process to establish the proportionality of new installations or upgrades to existing capabilities should be instituted

This recommendation applies specifically to the upgrade of the St Helier town centre system, to proposed introduction of ANPR and the expansion of body worn cameras by the SoJ Police. As a general principle, other public service providers should take an evidence-based approach to the deployment of their camera systems. This should comprise an unambiguous statement of what the surveillance equipment is intended to achieve, a clear and evidenced identification of the type and prevalence of the issue it is intended to address, identification of non-intrusive alternative strategies, and consideration of whether such less intrusive measures could be deployed for those ends (and only discounted if inadequate). New efficacy monitoring processes (recommendation 2) should also be drawn upon to make an objective and informed evidence-based decision over whether surveillance cameras provide the most effective response to the particular issue. Experience of practices in the UK and other EU countries could also be drawn on to inform this process.

4. A register is needed to log all access to surveillance camera control rooms

We recommend that all CCTV control rooms meet appropriate security standards and that a log of access to each control room is established. This log should include details such as the name of the visitor, time of visit, purpose and name an employee responsible for escorting the visitor. Visitors should be required to present a recognised form of identification before being granted access to a surveillance camera operations centre.

5. All external requests view surveillance footage should be logged

We recommend that all requests to view footage are recorded in a log, not just those incidences where footage is legally obtained for investigations. This log should apply to anyone not working, at that time, in the CCTV control room. The log should include details of the name of the person requesting footage, reason, time of request, and name of the person granting the request.

6. All camera systems operating in places to which the public have access should incorporate appropriate signage

The requirement to install signs should be embedded in the SoJ Data Commissioners CCTV Code of Practice. Signs should be clearly visible and located at the entry points to surveyed areas. Signs should include the following information:

- The operator of the system,
- The purpose of the system,
- A contact telephone number (and ideally a website/email address), and
- Information about any data matching taking place.

7. The States of Jersey should establish a census or register of CCTV cameras and systems

This could be achieved though a short one page extension to the data controller's annual submission to the Office of the Data Protection Commissioner. Data controllers should be required to specify the number of cameras they operate, their location and purpose, when the CoP was last updated and whether any data matching takes place. To ensure political oversight and to encourage public awareness the Data Protection Commissioner should provide an annual review of the prevalence of cameras and highlight any observable trends.

8. Introduce regulatory measures to govern the use of surveillance cameras in domestic residential settings

We recommend that new regulatory mechanisms be introduced to govern the use of surveillance cameras in domestic residential settings. This would be to reduce incidences where surveillance cameras from one residence survey another. It would also allow

mechanisms for the redress of grievances. Following consultation we suggest that existing planning regulations be adopted to accommodate the provision of CCTV in domestic residential settings. We also recommend that the Data protection commissioner produce specific guidance on the use of surveillance cameras in such settings.

9. Introduce a maximum data retention period of 31 days for public service providers

We recommend that image retention periods are limited to a maximum 31 days across public surveillance camera operations. This is common practice elsewhere in the UK and the EU. This maximum data retention period should be specified in the Data protection Commissioner's CCTV Code of Practice.

10. Introduce safeguards to ensure only appropriate and necessary data matching takes place

Data matching is a process that is relatively 'hidden' from public view. Whilst we do not want to obstruct the appropriate proportionate use of data matching it is important that the public are made aware of such processes, that they are captured by existing governance arrangements, and that safeguards are established to ensure unnecessary data matching does not take place. We recommend that any camera system that incorporates data matching as part of its purpose clearly specify this in the system's CoP and on appropriate signage. This should also be specified in the Data Protection Commissioner's CCTV Register of surveillance cameras and systems (recommendation 8).

11. All public and private operators using surveillance cameras in public places must establish a Code of Practice

It is standard practice elsewhere in the UK and beyond for a publically available Code of Practice governing the use of CCTV to be established where cameras operate in public places. Although this recommendation is a requirement of existing regulation it is evident that some operators in Jersey do not have a CoP and others have codes with are very old and/or are partially adhered to. We have recommended elsewhere that the proposed Data protection Commissioner's CCTV camera and system register includes the collection of data relating to the upkeep of individual operators CoP (Recommendation 8).

12. To bring the SoJ Data Protection Commissioner's CCTV Code of Practice in line with best practice

The SoJ Data Protection Commissioner's CCTV Code of Practice should be updated to take account of best practice elsewhere in the UK and beyond. Improvements we would point to include:

- A requirement for operators to include signage,
- To integrate the principle of 'surveillance by consent',
- A requirement for operators to engage in public awareness activities,
- A requirement for operators to periodically evaluate the performance of systems,
- A requirement for operators to establish a log or register of access to CCTV control rooms and footage,
- A requirement for operators to establish training in relation to appropriate levels of individual surveillance and live targeting,
- A requirement for operators to make the public aware of surveillance systems which incorporate data matching processes,
- To establish a register of cameras and systems,
- To provide more detailed guidance on the use of surveillance cameras in domestic residential settings, and
- To incorporate a definition of public space.

13. Establish processes to monitor compliance with the Data Protection Commissioner's CCTV Code of Practice

It is evident that a number of CCTV operators are not compliant with all aspects of Data Protection legislation in Jersey or the Data Protection Commissioner's CCTV Code of Practice. We recommend that the SoJ Data Protection Commissioner establish processes and mechanisms to ensure compliance takes place. The creation of a CCTV register (Recommendation 8) may assist in this process. CCTV operators should be reminded about the importance of compliance and the penalties arising from non-compliance. Individual CCTV operators should ensure compliance with their own CCTV CoP, and thereby compliance with the Data protection Commissioner's CoP, by identifying a named employee with the responsibility for ensuring compliance and the creation of processes to monitor compliance.

14. All operators of surveillance cameras in public places should undergo appropriate training

This training would include knowledge and skills associated with the processing of personal data, the requirement to collect performance related information and the actual process of undertaking surveillance. Training should explicitly cover ethical obligations, regulatory responsibilities, privacy, issues of data handling and protection, responsible subject monitoring and access requests. Training requirements should be set out in individual CoP and should be reported on in annual system reviews.

Bibliography

British Standards Institute (2009) *Closed Circuit Television (CCTV). Management and Operation. Code of Practice*. BS7958:2009 (September 2009), URL:

http://shop.bsigroup.com/en/ProductDetail/?pid=000000000030179151

Fussey, P. (2008) 'Beyond Liberty, Beyond Security: The Politics of Public Surveillance', *British Politics*, Vol. 3, No.1, pp.120-135

Fussey, P. (2007) 'An interrupted transmission? Processes of CCTV implementation and the impact of human agency', in *Surveillance and Society*, vol. 4, no.3, pp.229-256

Home Office (2013) *Surveillance Camera Code of Practice*. (June 2013), URL: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/204775/Surveillance_Camera_Code_of_Practice_WEB.pdf

Home Office (2007) *National CCTV Strategy* (October 2007), URL:

http://www.crimereduction.homeoffice.gov.uk/cctv/National%20CCTV%20Strategy%20Oct%202007.pdf

UK Information Commissioner's Office (ICO) (2008) *Code of Practice (revised edition)*, URL:

http://www.ico.org.uk/for_organisations/data_protection/topic_guides/~/media/documents/library/Data_Protection/Detailed_specialist_guides/ICO_CCTVFINAL_2301.pdf

States of Jersey Data Protection Commissioner's Office (2005) *Code of Practice and Guidance on the Use of CCTV*, St Helier: Office of the Data Protection Commissioner.

Webster, C.W.R., Töpfer, E., Klauser, F. and Raab, C.D. (eds.) (2012) Part 2: Revisiting the surveillance camera revolution: Issues of governance and public policy, *Information Polity*, Vol.17, No.1, pp1-6.

Webster, C.W.R., Töpfer, E., Klauser, F. and Raab, C.D. (eds.) (2011) Part 1: Revisiting the surveillance camera revolution: Issues of governance and public policy, *Information Polity*, Vol.16, No.4, pp-297-398.

Webster, C.W.R. (2009) CCTV policy in the UK: Reconsidering the evidence base', *Surveillance and Society*, Vol.6, No.1, pp.10-22.

Webster, C.W.R. (2004) The Diffusion, Regulation and Governance of Closed-Circuit Television in the UK, *Surveillance and Society*, Vol.2, No.2/3, pp.230-250.

Webster, C.W.R. (1996) Closed Circuit Television and Governance: The Eve of a Surveillance Age*. Information Infrastructure and Policy*. Vol.5, No.3, pp.253-263.

Welsh, B. C. and Farrington, D. P. (2002) *Crime prevention effects of closed circuit television: a systematic review*, Home Office Research Study 252, London: Home Office. URL: http://www.homeoffice.gov.uk/rds/pdfs2/hors252.pdf

The Authors

Professor Peter Fussey, University of Essex

Pete Fussey is a professor of sociology in the Department of Sociology at the University of Essex, UK. The Department of Sociology at the University of Essex is renowned for its research excellence and is currently nationally ranked in joint first position for the quality of its research. Professor Fussey's main research interests focus on criminology, security, social control and the city. He has published widely in the area is currently working on two large-scale ESRC and EPSRC funded research projects looking at counter-terrorism in the UK's crowded spaces and at the future urban resilience until 2050. His other work focuses on organised crime in the EU with particular reference to the trafficking of children for criminal exploitation (monograph due to be published by Routledge in 2014). Recent books include *Securing and Sustaining the Olympic City* (Ashgate) and *Terrorism and the Olympics* (Routledge). Professor Fussey has also worked extensively with practitioner communities, particularly the UK government and various policing constabularies, in the areas of security, surveillance and counter-terrorism.

Email: pfussey@essex.ac.uk

Website: https://www.essex.ac.uk/sociology/staff/profile.aspx?ID=1955

Professor William Webster, University of Stirling

William Webster is Professor of Public Policy and Management at the Stirling Management School, University of Stirling. He is a Director of the *Centre for Research into Information, Surveillance and Privacy* (CRISP) and Chair of the *Living in Surveillance Societies* (LiSS) European research programme. He is one of the UK's leading experts on the governance and practice of CCTV in public places and has regularly advised a number of public agencies, including the UK ICO and a number of UK local authorities, on the provision of CCTV. Professor Webster has published a number of research papers on CCTV. He is also an editor of the journal *Information Policy* and host of the *Scottish Privacy Forum*.

Email: william.webster@stir.ac.uk

Website: http://rms.stir.ac.uk/converis-stirling/person/11731

APPENDICE 1: Camera Surveillance Review Terms of Reference

Education and Home Affairs Panel: Review of CCTV in Jersey

Terms of Reference March 2013

The Prevalence of Camera Surveillance:

To establish the types and numbers and costs of CCTV and ANPR cameras and systems deployed in the States of Jersey.

To consider the extent of surveillance camera usage in Jersey by commercial enterprises and for domestic security

The Effectiveness and Impacts of Camera Surveillance

To explore the role played by CCTV and ANPR in policing, community safety, transport and in the criminal justice system.

To examine the possible societal consequences of camera surveillance.

Public Attitudes Towards Camera Surveillance

To assess the extent of public awareness of cameras surveillance in Jersey.

To examine any concerns about the operation of CCTV and ANPR in Jersey.

To consult stakeholders and the public on what information should be available to any individual wishing to know more about overt surveillance cameras and how this information should be made available.

The Governance of Camera Surveillance

To establish the effectiveness of current guidelines/voluntary codes of best practice and their operation

To establish the rights of access to information and camera footage by citizens and what rights employees have in relation to CCTV surveillance by their employers.

To consider whether there is a need to develop the formal regulation of the use of CCTV and ANPR.

Appendix Two: The prevalence of camera surveillance: States departmental survey

Dept	Number cameras/ recorders/ monitors	Stated purpose	Costs and date of installation	Annual Operating & maintenance costs
SOJP: Town Centre	23	Reduction, prevention and detection of crime and criminal activity Evidence gathering Policing events Search for missing/vulnerable persons	£345,000 1996 £245,000 2002 £180,000 2007	£68,500
SOJP: Custody	15	Assist in management of detainees Custody images sometimes required for evidential purposes Safeguard police, detainees and all others involved in the detention process Reliable record of initial reception Recording of condition and demeanour of prisoner Reduce incidents of violent and disorderly behaviour by detainees Discourage malicious complaints and allegations and assist in investigation of complaints and allegations Enhance security and safety of staff detainees and others	Included in above	Included in above
SOJP: Police HQ	4	Building and vehicle security	Included in above	Included in above
SOJP/JCIS: Airport	21	Prevention, reduction and detection of crime and criminal activity Assist with local/national security and anti-terrorism operations Production of evidential material Search for missing/vulnerable persons	£200,000 2000	£5,800
SOJP/JCIS: Harbour	6	As above	£20,000 1999	£3,800
JCIS Custody Suite	15	As above	£5,900 1999	None
JCIS ANPR	4	Record arrivals/departures of all vehicles in and out of island	£29,000 2008	£1,420
SOJP mobile ANPR	1	Automatic alerting of vehicles of interest eg suspected disqualified drivers	£25,000 2006	negligible
Fire and Rescue	4 3	Building Security On separate fire engines: safety of vehicles on emergency calls (Standard equipment on modern fire engines)	No record 2004 2010	(i) Maintained by Communications Services (ii) Fleet maintenance
Prison Service	244 1 ANPR	Staff and prisoner security and protection Perimeter and internal security monitoring Crime prevention	£887,500 20 years	£25,000
Harbour (separate	24	Prevention and detection of crime and security breaches	- 1996	Maintenance contract

from SOJP/JCIS CCTV systems)		Facilitate apprehension and prosecution of offenders Discourage delinquent and anti-social behaviour Assist overall management of buildings and facilities Assist in protecting security and operational staff while carrying out their duties Assist in safety, monitoring and control of maritime traffic Assist in safety, monitoring, control and movement of commercial cargo and passenger operations within the restricted Areas of the Port Assist in search and Rescue situations within the port and adjacent waters Assist in monitoring and control of restricted areas and boundaries to meet the security arrangements as described in the International Ship and Port safety Code and Port facilities Safety Plan		
Airport (separate from SOJP/JCIS CCTV systems)	45 recording 40 from previous CCTV systems monitoring only	Prevention, investigation and detection of crime Apprehension and prosecution of offenders Public and employee safety Monitoring security of airport premises and facilities	£15,355 -	£3,500
ESC: Primary schools	75	Reduce vandalism Deter intruders from entering ESC premises	Range of costs depending on nature of premises	Range of costs depending on nature of premises
ESC: secondary Schools	171	Reduce vandalism Deter intruders from entering ESC premises	As above	As above
ESC: Highlands	19	Reduce vandalism Deter intruders from entering ESC premises	As above	As above
ESC: Sports Centres	106	Reduce vandalism Deter intruders from entering ESC premises	As above	As above
Housing	54	Crime prevention and public safety	£62,000 2003	£1,342 inspections £8,000 maintenance
HSS	50	Protect Hospital and HSSD staff against violence and aggression Protect HSSD infrastructure and equipment; prevent and detect malicious damage/theft	Recorders; £3,600 Cameras: £15,000	Included within annual security budget
Planning: Met Office	1	Webcam: northern end of airfield to give indications of weather	£100	None
Social Security:	34	Safety in perimeter and public areas, including reception, entrances and exits, car parks Security as a deterrent to crime and investigation of crime Improve customer services – monitor queues	£11,200 2006	
TTS: EFW: La Collette	30	Site and process operation, H&S, site security, offences (including alleged offences) and	Installed as part of EFW project	£2,000

		personnel/employee administration	2011	
TTS: Bellozanne	12	As above	£45,000	£1,500
TTS: Oil Compound	6	As above	unknown	£500
TTS: Abattoir	9	Site security and animal welfare	£6,000 upgrade 2013	£400
TTS: Animal Incinerator	3	Site security, process monitoring	£3,000 2001	£200
TTS: car parks	187 4 ANPR	Security of site and personnel, enforcement of parking Regulations, monitoring traffic movement, detection and prevention of crime, H&S, and personnel/employee administration vehicle parking charges (trial ANPR period)	Unknown 2000	£7,500
TTS: Green waste	14	Site and process operation, H&S, site security, offences (including alleged offences) and personnel/employee administration	Unknown 2007	£1,500
TTS: Millennium Park	10	Security of site and personnel, enforcement of park Regulations, detection and prevention of crime, H&S, and personnel/employee administration	£33,000 2011	£1,500
TTS: HD park	8	As above	£24,000 2009	£1,000
Central market	6	Illegal entry to market when closed	£30,000 2004	£1,250
Morier House	12	Security of site users in hours and security of premises out of hours		
States Building	6	As above		
Maritime House	5	As above		
Magistrates Building	12	As above		
Probation Building	8	As above		
Cyril le Marquand	29	As above		

Total number of cameras 1308

Appendix Three: Public survey: summary of results

Introduction

The Education and Home Affairs Panel conducted an online public opinion survey on the Scrutiny website to explore public awareness and attitudes towards camera surveillance in Jersey. 46 responses were received between 25 June and 9 September 2013. This is clearly only a very small sample of public opinion. It should also be noted that respondents were self selecting – there was no attempt to provide a scientifically balanced representation of the population as a whole.

Section 1 About you

- 20% had an accurate knowledge of the number of cameras in St Helier Town Centre (20-29)

Section 2 Awareness of cameras in public areas

- 65% disagreed with the statement that CCTV surveillance in public areas in our Island today was excessive;
- 59% disagreed with the statement that public expenditure on CCTV cameras should be reduced;
- 47 % however said that they did not want to see any additional CCTV;

Section 3 Effectiveness of CCTV cameras

Public spaces

- 60% agreed with the statement that CCTV cameras in public spaces made them feel safer;
- 64% disagreed with the statement that low levels of crime in Jersey meant that CCTV in public spaces was unwarranted;
- 62% agreed with the statement that cameras in public areas helped to reduce crime and disorder
- 78% agreed with the statement that CCTV provides vital evidence in the prosecution of suspects/offenders

- 70% agreed with the statement that CCTV cameras in public places helped to deter anti-social behaviour and vandalism
- 63% agreed with the statement that CCTV cameras in public places helped the police to deal with incidents quickly

Retail

- 77% agreed with the statement that CCTV cameras in shops were effective as a means of deterring crime

Buses

- 71% agreed with the statement that CCTV cameras on buses protected both staff and customers

Schools

- 56% agreed with the statement that CCTV cameras in school classrooms and corridors helped to ensure pupil safety when they were not supervised in lessons

Homeowners

- 83% agreed with the statement that CCTV cameras were a useful tool for homeowners to protect their property

Workplace

- 63% disagreed with the statement that CCTV cameras were a useful tool for employers to monitor their employees

Section 4 Personal Privacy Issues

Public spaces

- 58% disagreed with the statement: 'CCTV cameras in public areas infringe my personal right to privacy
- 60% agreed that CCTV cameras in public areas posed no risk if you had nothing to hide
- 64% disagreed with the statement: the extent of CCTV surveillance in public areas in our island today is excessive.

Domestic

- 47% agreed that the presence of CCTV cameras near my home infringed my personal rights to privacy; 33% disagreed; 16% said it was not applicable

Workplace

- 55% agreed that the presence of CCTV in the workplace infringed my personal right to privacy; 31% disagreed; 10% not applicable.

Information

- 79% agreed that they should be informed when they were under surveillance

Access to data

- 93% agreed that they should be allowed access to data collected about them

Appendix Four: Key documents relating to the governance and regulation of CCTV

Recent years have seen the publication of many documents relating to operation, standards and data handling in relation to CCTV published by local authorities, national government and the private sector. This document lists some of the main publications.

Based on our two visits to Jersey, we are of the view that these three documents are of greatest relevance:

• **UK Information Commissioner's Office (ICO) Code of Practice (2008)**
http://www.ico.org.uk/for_organisations/data_protection/topic_guides/~/media/documents/library/Data_Protection/Detailed_specialist_guides/ICO_CCTVFINAL_2301.pdf

Particularly relevant are the sections on signage and how to effectively advertise the existence of CCTV surveillance in a given area.

• **Home Office Code of Practice (June 2013)**
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/204775/Surveillance_Camera_Code_of_Practice_WEB.pdf

This is the latest UK government guidance on CCTV operational practice. Amongst other obligations, the Protection of Freedoms Act 2012 created a statutory requirement for the establishment of (a) a 'surveillance camera commissioner' and (b) a CCTV code of practice. It only applies to public bodies but we feel the main principles could be embedded into the activities of private operators.

The most relevant section of this concerns the notion of 'surveillance by consent'. Page 4 also contains a useful definition of 'public place' that could be applied to Jersey. There is also considerable emphasis placed on accountability, transparency and responsibility – all areas that are relevant to Jersey.

• **UK National CCTV Strategy 2007**
http://www.crimereduction.homeoffice.gov.uk/cctv/National%20CCTV%20Strategy%20Oct%202007.pdf

This was the first attempt at creating a national co-ordinated approach to the operation of CCTV. The strategy was authored by the Home Office (National Police Improvement Agency) and ACPO. The emphasis here is the standardisation of technologies and administrative processes in order to maximise the effectiveness of systems. Whilst some recommendations have been superseded by the 2013 Home Office Code of Practice, the National Strategy sets out a number of clear principles for the operation of CCTV. We think that the information of the retention of data is particularly relevant for Jersey.

Other UK-focused documents include

• Surveillance by Consent Home Office Press Release (June 2013):
https://www.gov.uk/government/news/surveillance-camera-code-of-conduct-comes-into-force

- Home Office Consultation (Published March 2013): https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/118263/code-surveillance-cameras.pdf

- Home Office Response to Consultation (March 2013) https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/118266/response-surveillance-cameras.pdf

- Home Office Code of Practice under Protection of Freedoms Act 2012 (2013): https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/157901/code-of-practice.pdf

- Home Office Impact Assessment (2013): https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/157907/consultation-impact-assessment.pdf

- CCTV Operational Requirements Manual - May 2009 http://scienceandresearch.homeoffice.gov.uk/hosdb/publications/cctv-publications/28_09_CCTV_OR_Manual.pdf?view=Binary

- Retrieval of Video Evidence & Production of Working Copies from Digital CCTV Systems v2.0 - Oct 2008 (Provides a procedure and guidance to police technical staff wishing to identify the most appropriate method for retrieving video from any digital CCTV system) http://scienceandresearch.homeoffice.gov.uk/hosdb/publications/cctv-publications/66-08_Retrieval_of_Video_Ev1.pdf?view=Binary

- CCTV First Responder's Protocol - Aug 2008 (Basic "do's and don'ts" guidance leaflet for officers who are the first-on-scene at an incident from which CCTV evidence is required) http://scienceandresearch.homeoffice.gov.uk/hosdb/publications/cctv-publications/FirstResponse_22-Nov-06_v0.1.pdf?view=Binary

- CCTV and Imaging Publications (Link to the Home Office Scientific Development Branch publication list of CCTV related information) http://scienceandresearch.homeoffice.gov.uk/hosdb/cctv-imaging-technology/

- CCTV-and-imaging-publications http://scienceandresearch.homeoffice.gov.uk/hosdb/cctv-imaging-technology/CCTV-and-imaging-publications>

British Standards Institute

- BS 5979:2000-Code of practice for remote centres receiving signals from security systems http://shop.bsigroup.com/en/ProductDetail/?pid=000000000030043539

- BS7958:2009-Closed circuit television (CCTV). Management and operation. Code of Practice. http://shop.bsigroup.com/en/ProductDetail/?pid=000000000030179151

- BS8495:2007-Code of practice for digital CCTV recording systems for the purpose of image export to be used as evidence. http://shop.bsigroup.com/en/ProductDetail/?pid=000000000030156323

• British Security Industry Association: CCTV using IP Technology (2009)
http://www.bsia.co.uk/web_images/publications/form_235.pdf

Scotland

• The Scottish Government: Strategic report on Improving the Efficiency and Effectiveness of Public Space CCTV in Scotland: November 2009
http://www.scotland.gov.uk/Resource/Doc/294514/0091077.pdf

• The Scottish Government: The Effectiveness of Public Space CCTV: A review of recent published evidence regarding the impact of CCTV on crime - December 2009
http://www.scotland.gov.uk/Resource/Doc/294462/0090979.pdf

• The Scottish Centre for Crime & Justice Research: Public Space CCTV in Scotland: Results of a National Survey of Scotland's Local Authorities - December 2009
http://www.sccjr.ac.uk/documents/CCTVtog.pdf

Australia

• Managing CCTV Records (2010):
http://www.adri.gov.au/products/cctv_guideline.pdf

• National Approach for Transit Systems (2012):
http://www.infrastructure.gov.au/transport/publications/files/CCTV_Code_of_Practice.pdf

New Zealand

• Data Protection Commissioner's Report CCTV and Privacy (2009):
http://www.privacy.org.nz/assets/Files/Brochures-and-pamphlets-and-pubs/Privacy-and-CCTV-A-guide-October-2009.pdf

Canada

• Office of the Privacy Commissioner of Canada (2008). Guidelines for Overt Surveillance in the Private Sector
http://www.priv.gc.ca/information/guide/2008/gl_vs_080306_e.pdf

Legislation

Other relevant UK legislation which we have not referenced here would include the Data Protection Act 2008, the Human Rights Act 2008 and the Protection of Freedoms Act 2012. At the EU level there is the Data protection Directive. This is currently being reviewed and the revised directive, which may take many years to implement in Member States is likely to incorporate the concept of 'purpose limitation', that systems should only be sued for the purpose they are intended and which is specified.

Professor William Webster Dr Pete Fussey 4th July 2013

Appendix Five: Reflections on the Existing Code of Practice for CCTV

Introduction

There are a number of Codes of Practice (CoP) in operation in Jersey that relates to the provision of video surveillance cameras. The Data Protection Commissioner has issued a Code of Practice (2005) governing the use of cameras in public places. Additionally, every operator should have a publically available CoP. The reflections contained in this short paper relate to the CoP issued by the States of Jersey (SoJ) Data Protection (DP) Commissioner. CCTV Operates Codes should be complaint with the Code issued by the SoJ DP Commissioner.

General Themes

From the evidence supplied to the Scrutiny Panel it is apparent that some aspects of the CoP should be brought in line with best practice elsewhere in the UK and Europe, and that other elements of the existing CoP are not being adhered to by CCTV operators in Jersey.

Areas where the CoP could be improved are:

- **Signage.** The Code of Practice should contain a requirement to provide signage in publically surveyed areas. This is normal practice elsewhere. Detail should be provided on the key pieces of information that should be displayed on each sign.

- **Surveillance by Consent**. The CoP should contain something on the need to seek consent from the surveilled. i.e. signs for public and private spaces, and the need for consultation exercises for public camera installations.

- **Public Awareness.** The CoP should contain a requirement to make the public aware of the purpose(s) of CCTV and the location of cameras (etc.).

- **Evaluation.** The CoP should include a requirement for CCTV providers to evaluate the purpose and effectiveness of their systems. On page 10 the CoP states “It is important that the images produced by the equipment are as clear as possible in order that they are effective for the purpose(s) for which they are intended”. The theme of evaluation is picked up again on p.18. We recommend there should be a requirement that public CCTV operators undertake at least a minimum standard of evaluation to ensure their systems are effective and appropriately sited.

- **Access to Footage/Control Rooms.** The CoP should include a requirement to register access to control rooms and CCTV footage. Such records should be audited. Most UK CCTV control rooms restrict and log access to these areas. We have not encountered similar practices in Jersey.

- **Surveillance and Live Targeting.** The CoP should include a requirement for appropriate training and the audit of targeted surveillance. This is considered good practice elsewhere.
- There should be a statement on the acceptable length of time for following a suspect without any concrete grounds for reasonable suspicion.

• **Data Matching.** The CoP should include a requirement to specify where the matching of personal date takes place, with whom and for what purposes. This is a requirement of European data Protection law. In this respect, data should only be matched with named databases (i.e. ANPR images with the official vehicle licensing database) and not be matched with other unnamed databases. There needs to be a mechanism to regulate this.

• **Register of Cameras.** The CoP could include a register of systems/cameras. This would ensure greater transparency surrounding the proliferation and use of CCTV in Jersey.

Specific areas of the CoP.

• Areas not covered by the code of practice (p.7). Consider whether this statement "Security equipment (including cameras) installed in homes by individuals for home security purposes" should be omitted.

• The need for a code of practice (p.6.) The point about the inappropriateness of standards as a mechanism of regulation could be strengthened, i.e. standards are rather narrowly focused and do not really attend to a range of operational issues.

• Business requirements (p7-8). Could add a requirement to document the coverage of the cameras. Could also state that they are beholden to the same standards as operators of public systems.

• Domestic CCTV (p. 8.) "then the user should consult with the owners of such spaces if images from those spaces might be recorded." This could be strengthened to say "the user should seek approval from the owners of such spaces" and drop the clause "if images from those spaces might be recorded"

• P8. This could be strengthened: "If it is not possible physically to restrict the equipment to avoid recording images from those spaces not intended to be covered by the scheme, then operators should be trained in recognising the privacy implications of such spaces being covered (First and Third Data Protection Principles)."

• Fair and Lawful use of CCTV equipment. P.9. Signage. This could be strengthened considerably. Consider changing 'should' for 'must'. See the UK ICO report for clear guidance on what signs should look like and the information they should exhibit.

• Quality of the images recorded. P.10. The reference to 'tapes' is now outdated and should be amended.

• Retention of CCTV tapes (p.12). This could be more explicit. In UK public CCTV systems it is common for images to be retained for no longer than 28 days.

• Viewing of CCTV images (p13). "Monitors displaying images from areas in which individuals would have an expectation of privacy should not be viewed by anyone other than authorised employees of the user of the equipment (Seventh Data Protection Principle)." Should there be a log of these authorised employees?

• Staff training in the correct use of CCTV equipment (p14). Could add that managers have a responsibility to inform new staff and remind existing staff on an annual basis?

- Disclosure (p.15). The CoP contains this statement "All requests for access or for disclosure should be recorded. If access or disclosure is denied, the reason should be documented (Seventh Data Protection Principle)". But the scrutiny panel has revealed numerous incidences where this is not being followed. Perhaps this could be put in stronger terms, placing a requirement that all requests to review materials should be logged and this log should be made available to the Data Protection Office on request.

- P16-17. Subject Access. We have seen little evidence that much in this section is adhered to by data controllers.

- Glossary. A broadly conceived definition of public space could be added here.

Professor William Webster, University of Stirling
Professor Pete Fussey, University of Essex

30 August 2013

Appendix Six: Submissions and Public Hearings

Submissions

Mr. M. Dun

Tony Bellows

Data Protection Commissioner

Jersey Advisory and Conciliation Service

Chamber of Commerce

No-CCTV

Jersey Human Rights Group

Public Hearings: Witnesses

Data Protection Commissioner	26.06.13
Minister for Home Affairs	26.06.13
Acting Chief Inspector A. Williamson, States of Jersey Police	28.06.13
Minister for the Environment & Director, Development Control	28.06.13
Mr C. Farrier, Co-founder, No CCTV	18.09.13