States of Jersey Education and Home Affairs Scrutiny Panel

Review of Camera Surveillance

External Advisers' Final Report

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

Professor William Webster

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

Stirling Management School

University of Stirling

Stirling

FK9 4LA

Scotland, UK

CONTENTS

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

[1] 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.

- 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.