STATES OF JERSEY

CAMERA SURVEILLANCE IN JERSEY (S.R.1/2014): RESPONSE OF THE MINISTER FOR HOME AFFAIRS

Presented to the States on 18th February 2014
by the Minister for Home Affairs

STATES GREFFE

CAMERA SURVEILLANCE IN JERSEY (S.R.1/2014): RESPONSE OF THE MINISTER FOR HOME AFFAIRS

Ministerial Response to:	S.R.1/2014
Ministerial Response required by:	28th February 2014
Review title:	Camera Surveillance in Jersey
Scrutiny Panel:	Education and Home Affairs

INTRODUCTION

The Panel has examined developments in CCTV use in Jersey which are being led by the States of Jersey Police, namely the renewal and digitalisation of the Town Centre CCTV network, the introduction of body-worn cameras for Police Officers, and the proposal for a fixed Automatic Number Plate Recognition (ANPR) camera surveillance system around St. Helier. These and other issues are discussed in detail in the report.

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.

FINDINGS

	Findings	Comments
1	**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 adviser's report section 2.1).	Most members of the public recognise that Police CCTV cameras are there to prevent and detect crime and ensure public safety. It is recognised there is always room for increased public consultation and engagement in order to ensure greater transparency. The term 'surveillance by consent' underpins how public space CCTV systems are being used and developed. It is, however, recognised that the phrase may cause confusion by introducing a notion of consent beyond that exercised directly by individuals themselves on their own behalf. The provision of information is the first step in transparency and accountability. CCTV Cameras are strategically and overtly placed; they are not hidden but are there for all to see. Information

	Findings	Comments
		outlining the location of the Town CCTV system has recently been added to the States of Jersey Police website. People in public places should normally be made aware whenever they are being monitored by cameras and who is undertaking the activity. Signs indicating that cameras are operating can be displayed where appropriate. However, coverage of the Town Centre is extensive, which has the potential to result in an excessive amount of signage being placed around the Town Centre. The police are supportive of any framework that helps in the fight against crime and anti-social behaviour, while reassuring the public that cameras in public places are used proportionately and effectively.
2	**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 adviser's report, section 2.3 and recommendation 3).	The aim of the Town Centre camera system is to help reduce and detect crime and reduce the fear of crime. It also supports longer-term crime reduction strategies. This contributes to providing a safe environment for those living, working and visiting St. Helier. It is important that the use of camera systems should not be intrusive and should remain proportionate to the purpose for the surveillance in the first instance. It is recognised that public confidence and trust may be improved by a clear explanation outlining why monitoring of public space is considered legitimate and necessary. The National Decision-Making model is a fundamental element of training and forms the basis for the deployment and use of cameras. An assessment of lawfulness, proportionality and necessity remain key to police decision-making and ensuring actions are legitimate. Many of the issues raised are enshrined in Human Rights legislation, by which all officers and staff are bound.

	Findings	Comments
		Good practice dictates that any CCTV system should be periodically reviewed to ensure it remains necessary, proportionate and effective in meeting its stated purpose. The system operates fairly within the law and only for the purposes for which it is intended. It is utilised with due regard to the right of respect for privacy of the individual.
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).	A process of recording additional information on the use of CCTV will contribute to the dissemination of clearer information on the States of Jersey Police website. This will allow the public to have a more informed perspective.
4	**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 and 167).	The dissemination of far more information on camera systems, locations, policy and procedures, impact assessments, performance statistics and other management information, including reviews and audits undertaken, will hopefully generate increased public feedback. Increased consultation and engagement will provide an opportunity to identify any concerns; and influence the balance between public protection and individual privacy. Any extension of the Town CCTV system will involve wider public engagement, ensuring that the public's views about police camera systems are taken into account.

	Findings	Comments
5	**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 and 208 and adviser's report, section 2.2).	The States of Jersey Police recognise the importance of evidencing that the camera systems reflect an efficient, effective and economic way of enhancing policing and ensuring public safety; and that the cameras are sited appropriately. A procedure has been initiated to ensure the capture and wider dissemination of data to allow the public to assess the value of the system.
6	**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 adviser's report, section 2.11).	A UK Surveillance Camera Code of Conduct came into force in June 2013. A new local code of practice may help reassure the public that their civil liberties are being respected and enable them to challenge wherever they have concerns. It is suggested that there are already in place appropriate checks and balances; however, any further promotion of good practice and approved standards is welcomed.
7	**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	The current, ongoing, project is intended to replace and upgrade cameras which are over 15 years old, are no longer cost-effective or fit for purpose. Camera technology has developed in the years since the system was installed. The current upgrade and replacement is in effect a simple like-for-like 'swap' to ensure

	Findings	Comments
	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 adviser's report, section 2.5).	the recording of high-quality images. Work on the like-for-like replacement system is already underway due to technical issues with the existing system. A like-for-like recording solution has been purchased and installation is underway (completion end of February 2014). A process of continuous review of the Town camera system helps in assessing whether the locations of cameras remain appropriate and justified, and whether there is a case for removal or relocation. The use of a privacy impact assessment can help enhance public confidence that a system operator has taken into account the potential to interfere with privacy. Following discussion with the Scrutiny Panel, wider data collection on the use of CCTV was initiated in October 2013. This will allow the publication of increased statistical information on an annual basis.
8	**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	Automatic Number Plate Recognition (ANPR), like most police information systems, does involve an element of data-matching. By way of example, when conducting a vehicle registration check (number plate), the details of the registered keeper are drawn from a database administered by Driver and Vehicle Standards. Driving Licence applications are administered by the respective Parish Authority. In the absence of such data-matching, it would be difficult for the Police to quickly establish who owned a vehicle, or whether any offences were being committed. There are currently in place clear guidelines, policy and procedure relating to the use of Police data to ensure compliance with the Data Protection (Jersey) Law 2005. The States of Jersey Police purchased an ANPR system in March 2006 and it was fitted to an unmarked traffic vehicle. In January 2009, a further

	Findings	Comments
	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).	vehicle was fitted out with the same system. Both these vehicles have since been decommissioned, and in 2012 a Volkswagen Transporter van was fitted with one of the original systems. This vehicle is operated by the 24hr uniform shift. This equipment remains available for operational use. In effect, SoJP have been utilising ANPR since 2006 and continue to have it available. It is not at present being utilised for operational reasons. In order to reduce the impact on resources and increase capability, consideration is currently being given to the use of static ANPR similar to one operated at St. Helier Harbour in conjunction with the Customs and Immigration Service. This may involve the siting of ANPR cameras at key locations covering the arterial routes into/out of St. Helier. A static ANPR camera system is one that is located in a fixed position. National guidelines outline that an assessment should be conducted taking account of the following factors – • National security and counter-terrorism • Serious, organised and major crime • Local crime • Community confidence and reassurance, and crime prevention and reduction. In summary, when used in an appropriate and effective manner, ANPR has proved to be a useful tool in the detection of many offences. States of Jersey Police are currently considering the implementation of ANPR covering access routes around St. Helier. Whilst funding is available, a full business case has not as yet been produced. In assessing whether new static ANPR cameras are to be deployed, a process of further review and wider consultation is required.

	Findings	Comments
9	**Body-Worn Video Cameras:** The States of Jersey Police are trialling 6 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 that 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).	The States of Jersey Police are in the process of considering a business case for the continued use of Body-Worn Video. There are strong arguments to support the fact that the investment in Body-Worn Video has improved Officer safety, improved evidential gathering capability and quality. It has also enhanced Officer confidence and has the potential to deliver actual savings in terms of providing best evidence and reducing not guilty and reserved pleas and reducing malicious complaints. Details of the States of Jersey Police Body-Worn Video Policy will be available on the States of Jersey Police website.
10	**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 specifies 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 (adviser’s report, section 2.10 and recommendation 10).	It is contended that there are already appropriate safeguards in place in the form of the Data Protection (Jersey) Law and Human Rights legislation. A Code of Practice may assist in ensuring due consideration to these obligations and contribute to decisions relating to legitimacy and proportionality.
11	**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	CCTV footage has become an important investigative tool for Police. It is regularly used to investigate and solve crimes and has proven to be very useful in court when used as evidence. Establishing an accurate and comprehensive register that outlines the location of CCTV systems would

	Findings	Comments
	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 be comprised 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 adviser's report, section 2.7).	assist in identifying potential sources of evidence. It would also assist in ensuring the public is better informed about camera systems.
12	**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 monitoring 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 (paragraph 87).	It appears that there is a general consensus that society is content for young people to be monitored by cameras to ensure safety. It is, therefore, possible that such consensus extends more widely and includes camera monitoring in public areas such as St. Helier.
13	**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	The effectiveness of a camera system is dependent upon its capability to capture, process, analyse and store images of a quality which is suitable for its intended purpose. Whilst keen to ensure the provision of better quality images for use by the Police and in the criminal justice system, there is currently no intention at this

	Findings	Comments
	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).	stage to incorporate any additional functions (such as facial recognition or movement sensors).
14	**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).	It is only proper that those who may be most affected by the siting of Police cameras should have the opportunity to raise any concerns. This forms part of the accountability that underpins the concept of surveillance by consent. Guidelines are clear that cameras will not be used to look into private property. Officers and staff must demonstrate suitable knowledge of pertinent legislation and understanding of Force policy relating to CCTV. All recording in the Force Control Room is carried out in a regulated area. Routine access is restricted. Any access by other persons will be with the permission of the control room supervisor. To access the camera system, officers and staff are required to log into the system using an individual log-on code. This ensures appropriate checks and balances and an auditable process.
15	**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	The States of Jersey Police are reviewing their policy and procedure. Once finalised, the policy will be disseminated and published on the States of Jersey Police website.

	Findings	Comments
	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 and 184 and adviser's report, section 2.11).	
16	**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 all 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 pre-requisite of the upgrade to the current Town Centre system (paragraph 193).	The States of Jersey Police conducts specific training (Human Rights Legislation, Data Protection (Jersey) Law 2005, and National Decision-Making Model), all of which reinforce the importance of the right to privacy, processing data fairly and lawfully, and ensuring that police action remains justifiable, necessary and proportionate. All operators to be trained in their responsibilities so they are aware of the user's security and disclosure policies and the rights of individuals. All CCTV data is stored securely with access limited to authorised personnel only. The Force complies with guidance and adheres to 'best practice' outlined in the Association of Chief Police Officers' procedure and best practice.
17	**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	Images and information obtained from a surveillance camera system should not be kept for longer than necessary to fulfil the purpose for which they were obtained in the first place. The retention period will vary due to the purpose for the system, and how long images and other information need to be retained so as to serve its intended purpose. It is not, therefore, possible to be prescriptive about maximum or minimum periods. On occasions, there

	Findings	Comments
	(sometimes triple) than, say, London's Metropolitan Police, (paragraph 201).	may be the need to retain images for a longer period; for example, when investigating a crime, to allow the opportunity to view the images as part of an active investigation.
18	**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 adviser's report, section 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).	Whilst there is no specific legislation regulating domestic CCTV use, the Police will assess any complaints to assess what, if any, offences are revealed. The absence of legislation can on occasions prove problematic.
19	**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	There are procedures in place to respond to such requests. Individuals can make a 'subject access' request under Article 7 of the Data Protection (Jersey) Law 2005. Data includes images. Guidance on how to make

	Findings	Comments
	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 they may be required to provide heavy justification for their request (paragraph 246).	such a request is available to the public on the States of Jersey Police website.
20	**CCTV in the workplace:** There are legitimate uses of CCTV in the workplace: for example, in monitoring till transactions in bars and supermarkets, 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).	

RECOMMENDATIONS

	Recommendations	To	Accept/ Reject	Comments	Target date of action/ completion
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).	HA		Prior to the implementation of any new cameras, the Force will continue to review proportionality and effectiveness. This includes an assessment on whether the location of cameras remains justified in meeting the stated purpose and whether there is a case for removal or relocation. A privacy impact assessment would undoubtedly assist in assessing and identifying any privacy concerns.	
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).	HA		Relying on analytics to automatically monitor cameras and identify events of interest is in many cases much more effective than reliance on a human operator. However, functions such as line-crossing detection, motion detection, crowd or people detection, automatic track or zoom and facial recognition are not currently being considered. Any move towards incorporating such technology with the Town CCTV system should rightly be subject to public consultation. The new recording system is not capable of this without upgrade cost (and this has not been requested or budgeted for).	

	Recommendations	To	Accept/ Reject	Comments	Target date of action/ completion
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).	HA		Information is on the States of Jersey Police website. The process of review and dissemination of additional information continues. There is now a States of Jersey Police web-page dedicated to providing information on the Town CCTV system, policy and procedures. It is intended that the process of adding and updating information continues.	
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).	HA		Signage may be effective in regulating the use of CCTV and ensuring the privacy of the citizen. However, signage may increase anxiety about crime and disorder, or suggest a culture of criminality exists within St. Helier. It is suggested that rather than raising the profile of CCTV, signs would simply become absorbed into the environment of the Town to the extent that they go unnoticed. It is proposed that wider consultation and engagement with key stakeholders (residents, businesses and the Parish) take place before any decision is made. Planning permission and consent of building owners would be required to do this for Town Centre.	
5	**Recommendation:** Appropriate governance arrangements, an updated Code of Practice, and the introduction of auditable process should be	HA		Code of Practice to be updated to ensure compliance with UK and European standards and disseminated.	

	Recommendations	To	Accept/ Reject	Comments	Target date of action/ completion
	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).			CCTV Live view, Camera control and Playback fully audited in new recording system, due to be installed by end of February. Access/egress to/from the Force Control Room is by swipe card (audited).	
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).	HA		The Data Protection Law does not prescribe any specific minimum or maximum retention periods which apply to all systems or footage. Rather, retention should reflect the organisation's own purposes for recording images. Guidance dictates that images should be kept for as long as necessary to meet the purpose of recording them. On occasion, there may be a need to retain images for a longer period. Current retention times are set at 90 days for the Town CCTV system. System incapable of extending beyond 90 days without additional expenditure.	
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).	HA		Consideration will be given to how best to ensure property-holders are aware of the extent of CCTV coverage around the Town area.	
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	HA		ANPR cameras can only be deployed in the 'pursuit of a legitimate aim', such as assisting in the detection and deterrence of criminal activity. The	

	Recommendations	To	Accept/ Reject	Comments	Target date of action/ completion
	impact statement (paragraph 54)			process of reviewing and justifying ANPR will include consultation with stakeholders and an assessment of the impact. The ANPR system is regularly updated with registration details of vehicles driven by individuals the police are seeking, and then signalling an alert if one of these vehicles is captured by a camera.	
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).	CM		N/A	
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).	HA		ANPR is compliant with the provisions of the Data Protection (Jersey) Law 2005. There is a reasonable case to say that the use of a registered keeper database will enhance the ability to reduce offending and improve safety on the roads.	
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) .	HA		Current Force policy on the use of Body-Worn Video will be published on the States of Jersey Police website once its continued use has been ratified by the Chief Officer and the Minister.	

	Recommendations	To	Accept/ Reject	Comments	Target date of action/ completion
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).	CM		N/A	
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).	HA CM		Information to be presented to the Minister for Home Affairs and included in States of Jersey Police Annual Report.	
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	CM		N/A	

	Recommendations	To	Accept/ Reject	Comments	Target date of action/ completion
	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 adviser's report, section 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).	CM		N/A	
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).	CM		N/A	
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).	HA CM P&E		States of Jersey Police website updated to reflect this. The States of Jersey Police welcome the implementation of the draft code as a single source of advice and guidance on the use of camera systems in public places.	
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	HA CM		Information collected for one area of policing purpose may have value to another. Therefore, all police information should be treated as a corporate resource. The use of	

	Recommendations	To	Accept/ Reject	Comments	Target date of action/ completion
	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 (adviser's report, section 2.10 and recommendation 10).			ANPR is compliant with the provisions of the Data Protection (Jersey) Law 2005.	
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).	HA CM		A regular review of the proportionality and effectiveness of camera systems should assess whether the location of cameras remains justified in meeting the stated purpose and whether there is a case for removal or relocation. The States of Jersey Police are currently working with the Ports Authority to share cameras where possible (and hence reduce number).	
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).	HA		A review of by the College of Policing suggests CCTV is designed to change the environment within which crime occurs and makes for a small, but statistically significant, reduction in crime. Whilst the importance of collecting data is recognised, the process suggested would impose a disproportionate administrative burden. The Town cameras are located to monitor areas that either see the highest rate of footfall, are busiest in terms of the night-time economy. or are identified as 'potential hotspots' for crime or anti-social behaviour. If any of the Town cameras were not	

	Recommendations	To	Accept/ Reject	Comments	Target date of action/ completion
				considered useful or effective in supporting policing or safeguarding the public they would be removed or relocated.	
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).	CM		N/A	
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 adviser's report 2.13).	HA CM		The public expect CCTV to be used responsibly with proper safeguards in place. All officers and staff within the States of Jersey Police are trained. Effective policing depends on efficient information management. All officers and staff within the States of Jersey Police are well trained in the principles of data management, highlighting individual human rights and compliance with the law. There are clear policies and procedures in place that regulate how information is gathered, managed, used and how it is shared. There is a process of additional training for Force Control Room Officers, CCTV operators and those who manage them.	

	Recommendations	To	Accept/ Reject	Comments	Target date of action/ completion
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).	HA		In the development or review of camera systems, proportionate consultation and engagement with the public and partners will be an important part of assessing whether there is a legitimate aim and a pressing need, and whether the system itself is a proportionate response. Review last undertaken in 2011/2012. In line with a commitment towards greater transparency, there is a process of releasing increased information. It is intended to include this information in future annual reports.	
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 (Adviser's report, section 2.4).	HA		Already in place: • Swipe card for staff • Visitors signed in at enquiry desk.	
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	HA		There is policy in place to control how images and information are stored and who has access to them. • Authority to view process in place • New recording platform fully audited • Viewing of any CCTV linked to case file also logged.	

	Recommendations	To	Accept/ Reject	Comments	Target date of action/ completion
	person granting the request (Adviser's 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 (adviser's report).	HA		The retention period was initially set at 32 days. Following consultation with other stakeholders, it was considered that an extension to 90 days better served the interests of those within the judicial system. In effect, a delay in defendants receiving legal advice had the potential to negate the ability to recover CCTV evidence to support the defence. It was therefore considered that an extension to the retention period would best serve the interests of justice. Custody CCTV exceeds the standard 90 days in some areas.	
27	**Recommendation**: The Panel recommends that the Minister for Planning and Environment gives serious consideration to reviewing the classification of CCTV as permitted development and follows the example of Scottish legislation on this matter (paragraph 236).	P&E		N/A	
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).	CM		N/A	

CONCLUSION

Many of the recommendations contained above are for the Minister for Home Affairs. Some are for the Minister for Planning and Environment and some are for the Chief Minister. However, as some of them relate to more than one Minister, the entire list has been circulated for consideration.