Human Rights Commission
2nd Floor – Smith Road Centre
P.O. Box 391 Grand Cayman KY1-1106
(345) 244-3685

Eric Bush
Deputy Chief Officer (Uniformed Division)
Portfolio of Internal and External Affairs
3rd Floor Government Administrative Building
Grand Cayman
CAYMAN ISLANDS

25 August, 2010

Via E-mail: eric.bush@gov.ky

Dear Mr. Bush,

Thank you for your e-mail via the Secretariat dated 11 August, 2010 in which you requested the Commission's comments and feedback on the Working Group on CCTV's Code of Practice.

The methodology behind the use of CCTV is expected to reflect the Government's commitment to the fundamental right to privacy under the European Convention on Human Rights [Article 8] in addition to individual's rights, freedoms, and responsibilities embedded within Part I of the Cayman Islands Constitution Order. The biggest concern from a human rights point of view is to ensure that the use of CCTV is subject to statutory regulation and some form of statutory based licensing system. Without the implementation of a comprehensive data protection law to address the diverse nature of CCTV, a code of practice on its own is generally not considered a legal framework sufficient enough to support the delicate process of sustaining compatibility between human rights and the operation of CCTV.

The right to privacy is generally guaranteed by Article 8 which says that "everyone has the right to respect for his private and family life, his home and his correspondence." Legal case history has shown that Article 8 has been interpreted widely and applied to a broad range of circumstances. It has, for instance, been used to cover telephone tapping and the use of bugging devices; it has been applied to prisoners and their right to send and receive private communications; it covers sexual life, so that a prohibition on homosexual acts in private between consenting adult partners has been held to be an unjustified interference with the right to privacy. More recently, it has been successfully argued in several environmental cases including a case where a chemical factory created a health hazard to the local populous.

Although CCTV itself has yet to be the subject of a case coming before the European Court, it has generally been accepted that the concept of CCTV in both instances of its private and public contexts generates human rights implications with respect to two inherent characteristics: 1) The surveillance role and 2) the information-gathering role.

In its surveillance role, CCTV will usually be operated overtly with the cameras being placed in public places or in places where the public have free access, such as a shopping mall. The European Court has made it clear that people are entitled to rely upon a degree of expectation of privacy even in public places, although this is clearly less than when in private.

In its information-gathering role, CCTV has direct implications for what is referred to as 'informational privacy rights'. This is largely covered by data protection laws. While the Cayman

Islands Data Protection Working Group has been established it does not seem to deal expressly with CCTV or the protection of the right to privacy.

The Article 8 Tests

Once it is established that technology such as CCTV has the potential to interfere with privacy rights, Article 8 (as a qualified right) requires that three tests have to be applied if the interference is to be lawful.

First, the interference must be undertaken 'in accordance with the law' i.e. there must be a statutory legal basis for allowing the state to interfere in the particular way alleged; it is not considered acceptable to operate merely following a voluntary code of practice or internal guidelines. The best example of this concerns telephone tapping. Until the mid-1980's telephone tapping by the police was governed by internal guidelines and police standing orders. The European Court in the 1984 Malone case ruled that this was not good enough: any conduct by the state which is potentially intrusive has to be the subject of controls in an Act of Parliament and this law must be clear and easily accessible to ordinary people. As a result the 1985 Interception of Communications Act was introduced.

Second, to be lawful the aim of the interference must relate to an exception found in Article 8 which allows the right of privacy to be restricted i.e. in cases such as protecting national security, public safety, public health and morals, the rights of others or preventing public disorder or crime. This list is intended to be exhaustive; states cannot add restrictions that are not listed in Article 8.

Third, the restriction is subject to demonstrable justification in relation to fulfilling a pressing social need and the response being proportionate to the said need. It cannot, therefore, just be asserted that the interference is necessary to protect public safety, there has to be concrete evidence that there is a genuine threat to public safety and that this is an appropriate way of responding. The assessment to identify the concrete evidence needed should be based on fundamental concepts such as *proportionality, legality, accountability, necessity and subsidiarity.*

Proportionality

Proportionality refers to balancing the level of threat or risk to public safety against that of privacy rights through forethought of the number of cameras used and the manner in which the cameras are used. In other words, the system's design and application ought to commensurate to the seriousness of the risks and offences in which it is aimed at protecting against. In turn, as a general principle of avoiding infringement against privacy rights, consideration should be given to all available options capable of achieving the objective, and selection should be made of the least intrusive instrument or combination of instruments.

Legality

Legality relates to the assurance that CCTV operators are comprehensively aware of, and committed to, the system's binding CCTV Legislation as well as the Code of Practice and Procedures, including matters relating to, although not limited to: Human Rights, Data Protection, The Criminal Procedure Code, The Police Law, and The Evidence Law.

Accountability

Ambiguity should be minimized from an accountability perspective by acutely demonstrating that monitoring is being carried out for appropriate reasons, and processes should be governed by a publicly available Code of Practice and Procedures reflective of legislation.

Necessity

In evaluating the element of necessity, public space surveillance by CCTV is envisioned not as a panacea but rather as a tool to assist with enhancing public safety, deterrence of criminal activity and detection of crime. On the preceding grounds, arbitrary surveillance and application of unjust interference processes cannot be construed as necessary within a democratic society. For this reason, data controllers, operators, and public authorities must be able to justify any infringement of rights, and adequately defend infringement in parallel with a supporting legal regime.

Subsidiarity

The element of subsidiarity is linked with a platform that affords CCTV operation the opportunity to minimize interference with the privacy and the rights of the individual, and conform to enforcement tests through devolved courts.

Legal Challenges

In the opinion of the HRC, CCTV under the Code of Practice in the Cayman Islands may be vulnerable to a legal challenge as failing the Article 8 tests in two broad scenarios.

First, and foremost, is the fact that the setting up of CCTV systems is not subject to any statutory regulations. Many argue that a correct interpretation of Article 8 requires that the state has a positive obligation to regulate all CCTV systems both public and private because of their potential to interfere with privacy rights. A number of European countries have recently introduced such regulations. In Denmark, for instance, all CCTV systems are subject to a licence being granted which must take account of people's right to privacy. Also, conditions may be attached such as where the camera is placed, how it is monitored and whether, for example, it can ever be combined with an auditory facility. A special licence is required if video recordings are to be retained particularly for crime purposes. The Science and Technology Committee of the House of Lords strongly supported the need for a regulatory scheme for CCTV in a recent report earlier this year

Secondly, it is arguable that neither the Confidential Relationship (Preservation) Law (1995 Revision) nor the Proposed Data Protection Law (as it stands now and when it comes into force) may be able to provide sufficient 'Article 8 safeguards' to cover some of the more advanced technologies that can be used in combination with CCTV. These technological developments are likely to introduce new and more intrusive uses for CCTV material i.e. not just as a tool to prevent crime, but instead to detect it. An example of this is when CCTV footage is combined with facial recognition's systems to identify people. This is already in use in other situations, such as football grounds. Perhaps, as importantly though, are the moves to create near-national pictorial databases by way of the new driver's licence (which has an attached photograph) and the passport photograph. These will provide huge databases against which CCTV images can be compared. This suggests that high-street CCTV system potentially offer unique surveillance opportunities. Although the new Data Protection Act is designed to cover the processing of CCTV image data, it is not specifically designed to deal with sophisticated data-matching processes carried out on a large scale.

General Comments on draft CCTV Code of Practice

5. DATA PROTECTION

5.1 *It is envisaged that the primary legislation that will regulate CCTV will be a Data Protection Law. A Data Protection Committee has already been established in the Cayman Islands and has been tasked with producing a Draft Data Protection Bill. It is anticipated that the eventual Data Protection Law will prescribe how personal data shall be processed, including how personal data shall be obtained, held and shared to ensure that CCTV surveillance is fair, necessary and proportionate to the stated aims of the system.*

5.2 *It is anticipated that the proposed Law will require that both public and private CCTV systems register with the Information Commissioner's Office or other regulatory body (which is likely to be established under the proposed Law). It is expected that the regulatory body so established will be tasked with issuing an overarching National CCTV Code of Practice that would be applicable to both public and private CCTV surveillance.*

5.3 *It is expected that the Law will also provide a framework for the proper handling of images captured by CCTV cameras following internationally recognized data protection principles. Those principles which will be applied to this Code of Practice are listed at clause 2.5, above.*

5.4 *When the Data Protection Law comes into force, this Codes of Practice should include a statement of compatibility with the Law. For example the Code of Practice may need to state whether the CCTV scheme is registered with the regulatory body established under that Law. If the scheme becomes registered at any time after installation of the system, a statement to this effect should be included in the Annual Report for that year and added to the Code of Practice.*

Comment: In the view of the HRC this section of the draft Code of Practice seems to have a confused identity and purpose. On one hand it sets out what "should" happen or what "shall" happen but on the other it talks about the proposed Data Protection Law, an overarching National CCTV Code of Practice and anticipated changes to the draft that will be reviewed once the law has come into force. Section 5 as a whole gives rise to a concern regarding the time line between the use of a public CCTV system and the implementation of the binding legislation.

7.13 *However, an exception may arise where public CCTV surveillance is carried out specifically for the purposes of prevention or detection of crime and apprehension or prosecution of offenders, pursuant to an investigation being carried out by RCIPS and in keeping with its policy pertaining to covert surveillance. SUCH COVERT SURVEILLANCE IS NOT COVERED BY THIS CODE OF PRACTICE.*

Comment: Covert surveillance does not contravene the individual's right to privacy under Article 8 of the European Convention of Human Rights (ECHR), providing the level of covert surveillance is not disproportionate to achieving its aims. What is RCIPS' policy pertaining to covert surveillance? If ICT message interception is guided by ICT Law s75, has consideration been given to a law necessary to provide legitimacy to covert video surveillance? If covert CCTV activity by police (and presumably other public agencies such as Immigration) is not guided by this code of practice, is, for example, the RCIPS code pursuant to a law with prescriptions for authorization, documentation of evidence to engage covert recording (necessary and proportionate), parameters, and expiry time/date of the authorization?

7.18 *A Procedure Manual containing the day-to-day instructions for running the system will be put in place. Whereas the Code is the policy document and is not subject to change too often, the Procedure Manual may change and develop in line with changes in routine and practice. The Manual will contain a list of aims and objectives, details of access to (and control of) monitoring areas, the structure and staffing of the Control Room, record keeping, information on the actions of operators, crime investigation records, image management, partnership protocols, legislation updates and notes on the development of the CCTV system. Any part of this Code of Practice which is procedural in nature will be reproduced and expanded upon if necessary in the Procedure Manual.*

Comment: This section is much like section 5 where there is the possibility of confusion as it talks about a Procedure Manual coming into force which will also lead to changes to the current draft.

8.13 *Except where used for training or demonstration, there should be no public viewing of the monitors. There must be careful selection of any material to be used for such purposes to ensure data protection principles are not breached.*

Comment: Under no circumstances should recorded material be released for commercial sale of material for training or entertainment purposes.

9.4 *Guidance and training are critically important aspects of the operation of CCTV, and they should be given adequate attention. The most neglected aspect of training consists of learning how to identify suspicious behaviour, when to track individuals and groups, and when to take close up views of incidents or people. This is often assumed to be self evident, or left to common sense. The informality of these processes leaves unexamined the predisposition of CCTV operators to consider some people or types more likely to commit crime than others, which in turn leads to inefficiency and discrimination. Adequate guidance, training, supervision and monitoring of staff should therefore be maintained.*

Comment: The process of using the system to "track individuals and groups" who are unaware of such tracking, is arguably covert operation. The process of identifying suspicious behaviour should avoid influence based on operators' discrimination, either consciously or unconsciously, on the grounds of aspects outlined in the Constitution- sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, age, mental or physical disability, property, birth or other status.

10.2 *General recorded data should be retained for a maximum of 60 days then the data should be electronically purged.*

Comment: Thought should be given to the semantics - should or will? If data 'should' be retained for a maximum period of 60 days and thereafter not purged, who is liable for the breach? Would data be considered legitimate after the specified period of 60 days if it is not purged accordingly? Are embedded automated processes foreseen as a solution to ensure that data is purged in accordance with the code, thus alleviating the need for EMC operators to engage in a time-consuming process of manually purging data and risk a breach of the code?

11.7 *The Portfolio of Internal & External Affairs shall be responsible for ensuring that effective independent evaluation of the CCTV System is undertaken periodically. This should include as a minimum:*

(a) Assessment of impact upon crime
(b) Assessment of neighbouring areas without CCTV
(c) The views of the public
(d) Operation of the Code of Practice
(e) Whether the purpose for which the scheme was established still exists and if not would the removal of the CCTV System cause a return of crime to the area.

Comment: Will such evaluations include breaches of security / code of practice; breaches would almost certainly have an effect on the evaluation of the (a) to (e). Will such evaluations test applicability of CCTV in criminal / civil cases in which personal data was obtained, used, retained, disposed, etc. in accordance with the legal regime and the code of practice?

12.4 *The Electronic Monitoring Centre's Log should be retained as an exhibit, and be produced with statements if they form part of the evidence in a case.*

Comment: Private information of individuals not concerned with a particular case must be redacted from the exhibited log.

12.6 *Recordings of an incident or alleged crime that is likely to be used as evidence in any judicial proceedings is sub judice and under no circumstances should be shown to any unauthorized person(s).*

Comment: Recordings in general should not be shown to any unauthorized person(s), not simply recording of an incident or alleged crime likely to be used as evidence in court.

13.1 *When it becomes apparent that a recording may have material of evidential value, two copies of the data will be made and placed on a CD/DVD or other approved media. The CD/DVDs will be initialed in ink by the Electronic Monitoring Centre staff member who made the copies. One copy will go to the RCIPS officer assigned to the case. The second copy shall be kept at the Electronic Monitoring Center in secured storage. Both copies should be clearly and uniquely labeled, sealed and treated as evidence.*

Comment: Can the CCTV operator / manager act on discretion or is a formal standardized written request by RCIPS or other legitimate party required prior to copying data for this reason? If copies are made because it appeared that the material is of evidential value yet it is never required for court purposes, how long are the copies retained by EMC? In the instances where copies are distributed to RCIPS via CD/DVD, consider, as policy, use of Write Once Read Many CD-R / DVD-R for integrity purposes.

13.4 *If it is necessary to produce copies of recording for judicial proceedings, it should be recorded in the Electronic Monitoring Centre Log how many official certified copies have been made, their reference number and who has possession of them. Copies should only be made for evidential purposes, and accessible to the RCIPS, the Attorney General, defence solicitors and other prosecuting authorities. Each copy shall be individually marked. Copies can only be produced by the CCTV Administrator or under his direction or by permission of the Attorney General or his appointed representative.*

Comment: Maintaining the integrity of images removed from a hard-drive for evidential purposes is vital. Video and still frame images must be protected at the earliest opportunity. Alteration or erasure can be prevented by designating the image file as read only.

13.5 *It is essential that copies taken from evidential recordings do not pass to public circulation. No copy of a recording within the possession of the CCTV Administrator will be disposed of without first being electronically wiped or destroyed. All copies taken from evidential recordings are to be returned to the CCTV Administrator upon request and the CCTV Administrator will undertake to electronically wipe or destroy them.*

Comment: Will a log be created to document wiping / disposal / destruction of a copy? Are such "logs" electronic in nature with technological safeguards?

14.3 *An investigating officer may show a video or still image of an incident to the public at large for the purpose of recognising or tracing suspects.*

Comment: Will such video or still frames be edited to protect the identity of data subjects who are not under any reasonable suspicion but are captured in the video or still frame (collateral intrusion)?

15.3 *The showing of CCTV footage to local members of the public including local trade and business people as part of a marketing strategy to raise ongoing financial support through sponsorship or other means may be done.*

Comment: Showing CCTV to such parties does not guarantee financial support, albeit the guarantee of financial support may not justify compromising individuals' identity or privacy.

15.4 *Recorded data may be viewed by anybody carrying out independent evaluation of the scheme.*

Comment: Minimum standards (criteria) may be beneficial for identifying suitable personnel to carry out independent evaluations; such standards promote quality control and assist in avoiding systematic conflicts-of-interest.

16.2 *Information must be published about the manner in which an individual can make a complaint about any aspect of the scheme. Particulars about how to make a complaint, the name and address of the person to whom the complaint should be made, and of their responsibility in handling the complaint, should be published in the form of a leaflet and posted on the Government's National CCTV Programme website.*

Comment: Can complainants expect a written response from the investigatory authority, and is there a specified timeframe for resolving a complaint?

16.4 *Breaches of the Codes of Practice and of security must be subject to proper investigation by, in the first instance, the person appointed to conduct the audit. This person shall be responsible for making any recommendations to remedy any breach that is proved.*

Comment: This Section deals with breaches of the "Codes" (query if there are to be more than one) which is critical when considering the protection of the right to privacy, however the content of this section is almost meaningless in this regard. The statement is more appropriate to describe the Government's attitude or policy to the future regulation of CCTV. What obligation in the code or law does Government have to remedy a breach or make necessary operational improvement regarding identified instances of interference beyond the parameters of law?

17.2 *When the Electronic Monitoring Centre is not staffed it will be locked. It is important that access to the Monitoring Centre is controlled to ensure that the integrity of the recordings is maintained in accordance with the Code of Practice.*

Comment: Responsibility in preserving the security of information is paramount; are advanced technological safeguards being considered to prevent compromise of the EMC and the data stored therein, i.e. biometrics?

Conclusion

The HRC is satisfied that the Government has begun to approach this matter in a positive way. An overall comment on the CCTV Code of Practice is that the content of the document is broad and some areas are very confused.

It seems clear that the UK Human Rights Act, by incorporating a right to privacy into UK domestic law illustrates the potential implications for CCTV systems especially those run by public authorities. In the Cayman Islands, Article 8 of the Bill of Rights will mean that the government will be obliged to introduce specific statutory regulations and controls over CCTV.

The HRC expresses grave concern with 1) hastening to begin using the public CCTV system due prior to the implementation of the binding CCTV legislation; and 2) the fact that the Draft Disclosure of Confidential Information (Regulation) Law does not cover data protection related to CCTV in any form.

It is also be noted that there is currently a proposal for both a Data Protection Law (as referenced in both the CCTV Code of Practice and the 11 June, 2010 Memorandum from the Data Protection Working Group) and what is suggested to be an interim Law which is currently in draft form, entitled the Disclosure of Confidential Information (Regulation) Law. The objective of the latter law is to repeal the Confidential Relationship (Preservation) Law (1995 Revision) which is currently in force. The HRC would caution that if the interim law is enacted as currently drafted, it will not fulfill the requirements of data protection in regards to CCTV and thus a complete Data Protection Law must be expedited as a matter of priority, prior to CCTV being introduced any more widely.

Although we have provided extensive notes on the Draft CCTV Code of Practice this project must take place under the auspices of a collaborative approach and thus in order to provide the most useful of comments we would need to collectively review the entire package of documents related to the use of CCTV including:

1) a more defined and updated National CCTV Code of Practice;
2) a Draft National CCTV Procedures Manual;
3) in so far as it is intended to apply to CCTV and to protect the right to privacy, the Draft Disclosure of Confidential Information (Regulation) Law (as the interim legislation); and
4) the Draft Data Protection Law.

For your information the HRC has sent initial correspondence to David Archbold, Chair of the Data Protection Working Group, expressing an interest in being a part of their group in order to assist in the smooth implementation of the public CCTV system.

We hope that our comments and suggestions will assist the CCTV Committee to move ahead with their work to lawfully begin using a public CCTV system in the Cayman Islands.

Kind regards,

Richard Coles
Chairman, Human Rights Commission

cc: Deputy Governor