February 2008 Forum – Minutes Extract
CCTV Compliance – Legal Perspective

Kenneth Mullen (Sheppard and Wedderburn LLP)

· Data Protection Act 1998 - UK Information Commissioner (ICO)
· Private Security Industry Act 2001 (Scot 2007)
· Human Rights Act 1998 (ECHR Article 8: right to private and family life)

With regards to human rights he commented on the Peck case of 1997, where Mr Peck was caught on camera (Brentwood Council) trying to commit suicide. Images of this were subsequently passed to the media, without his face being blurred. This case was raised by Mr Peck at the European Court of Human Rights, after a national case failed.The Regulation of Investigatory Powers Act (RIPA) 2000 gives controls on covert surveillance and the Freedom of Information Act 2000 gives us the 'right to know'.

The Private Security Industry Act 2001 [Scottish Order 1/11/07] states that a 'public space' surveillance licence is required from the Security Industry Authority (SIA) by security contractors, directors/partners in security firms and employees contracted to consumer (e.g. shopping centre)**.** Working without such a license and/or using/supplying unlicensed security staff is a criminal offence.He stated that the Data Protection Act 1998 (DPA) applies to the processing of personal data by data controllers on equipment in UK. Personal data includes datathat identifies a living individual (or is likely to be used with other information that cando so); and that may affect an individual's privacy. The definition of Equipmentincludes CCTV systems (CCTV for private domestic use will usually be DPA exempt)Data Processing includes the capture, storage, retrieval, onward transmission (and disposal/destruction) of data.

He clarified the following DPA Terminology:
· The Data subject is a living individual whose data is processed. The Monitoring of employees is covered (as well as the public)
· The Data controller is the organisation (not an employee) determining the purposes and means of data processing. DPA obligations fall directly on the data controller and the Controller has to register or maintain a 'notification' of all their processing activities with the ICO. Failure to do this properly is a criminal offence.
· The Data processor processes data only under the controllers' instructions (e.g. outsourcing of data hosting/archiving), has no direct obligations under

DPA; but the data controller must appoint the processor under written contract with certain security guarantees.

He then covered the Eight Data Protection Principles under the DPA which state that personal data must be:
1. Fairly and lawfully processed
2. Obtained only for specified, explicit and legitimate purposes
3. Adequate/relevant/not excessive
4. Accurate and kept up to date
5. Kept for no longer than is necessary
6. Processed in accordance with rights of individual
7. Kept secure (taking appropriate technical/organisational measures)
8. Not transferred outside EEA unless adequate protection in place

He explained what this means for CCTV as defined in the ICO CCTV Code of Practice (January 2008). The ICO's interpretation of DPA as it applies to CCTV operators states that there are 'Key issues' for business to follow**.** Failure to follow this code may (and the key word is 'may') indicate that an organisation is not complying with the DPA Principles. The penalties' for being in breach of the DPA (which are currently under review) are:
· a fine for processing causing unwarranted distress/damage
· Investigation/Enforcement action by the ICO
· potential public censure/undertakings
· criminal penalties for unlawful obtaining/disclosure without a controller's consent (usually employees)

Headlines for CCTV Controllers under the ICO Code of Practice are:
· Administration: Organisational controls and procedures
· Selection and siting of CCTV: e.g. not overlooking another's private property
· Use of equipment: To ensure quality and accuracy
· Recording/storage/disclosure of images: e.g. kept securely and for no longer than required
· Responsibilities: CCTV 'notices' in surveillance areas and Subject Access Requests (individual's right to obtain personal data relating to themselves)
· Control; Ensuring continuing legal compliance and staff training
Other Legal Issues are:
· Monitoring of Staff (App 3 of ICO Code): This is legal but consider staff awareness, system purpose and proportionality/intrusiveness
· Engaging CCTV Contractors/Contract Staff. Under the DPA clients and system operators must establish who is data controller/data processor and must have a written contract in place ensuring the 'data processor' gives sufficient security guarantees with regard to the reliability of staff / rights to verify compliance.
He summed up by saying that CCTV is a compliance/risk management issue and reasonable care must be taken to organise and control affairs responsibly and effectively, with adequate risk management systems.

CCTV should be viewed in the context of an organisation's overall information management strategy/risk oversight covering:

· The protection of organisational data, records and premises (includes CCTV and images)
· Clear processes for installation/operation/control
· Responsibility for oversight within organisation
· The Training/management of staff/external contractors
· Procedures to manage incidents efficiently/effectively·