

Private and public sector bodies widely use CCTV for security. Most will be aware of the need to control access to CCTV images and limit it strictly to authorised persons. Even individuals who are in public places have a right to have their privacy respected – a depressed man in Brentwood with a knife was found by the European Court of Human Rights to have had his rights infringed when the CCTV image was published (**Peck v United Kingdom** (2003))

Material published by the Information Commissioner yesterday suggests the office will take an interest if material from CCTV is distributed, even to those taking part in a surveillance process: the Information Commissioner required a video sharing website to debar access to CCTV images to those within a 30 mile radius of the cameras. The required procedures also included encrypting the transfer of CCTV images, putting in place an audit trail for viewer activity and ensuring checks are carried out on registered viewers.

CCTV users will therefore need to make sure that any off-site surveillance is only undertaken by reputable employees or contractors; and to check other procedures such as those by which recordings are destroyed in a timely fashion in compliance with the Data Protection Act. There is also a more general point, that personal data and indeed confidential information ought to be encrypted where there is a risk of losing laptops, memory sticks etc or servers being hacked.

For more details contact Nigel Urwin or Claire Morgan