ESSENTIAL GUIDE

BODY WORN CAMERAS AND THE LAW

Protection of Freedom Act 2012 - The Code of Practice for Surveillance Camera Systems

What UK legislation governs the use of body worn video technology?

Introduction

The Protection of Freedom Act (POFA) of 2012 is a wide-ranging piece of legislation. It embraces a raft of measures with significant implications for the rights of the individual. It was seen as an attempt by the coalition to rebalance some of the laws introduced by the previous government that they believed conflicted with civil liberties. Some of the key areas addressed include the DNA database, detention without charge and police stop and search powers.

Of critical interest to our industry is the Surveillance Camera Code of Practice (SCCP), prepared under the auspices of the POFA, along with the creation of a Surveillance Camera Commissioner. This position is currently held by Tony Porter and his role is to promote the code and review its operation and impact.

"Surveillance cameras are no longer a passive technology" the SCCP concedes. It acknowledges that surveillance is now proactive and capable of making detailed records and precise identifications; from the mass surveillance of ANPR (Automatic Number Plate Recognition) to the localised engagement of body cameras. Body camera technology is now routinely employed within law enforcement and adjacent sectors and it is sophisticated and portable. It is undoubtedly a game-changer and this has aroused intense public debate. Surveillance is no longer a remote spectator, but an engaged and often influential presence.

The SCCP does contain a section specific to body camera technology, however anyone responsible for the collection and retention of personal data should have due regard for the full guidelines.

The full document can be accessed from here, however we will take a look at some of the points more salient to us and our industry below.

Is the code law?

The code is designed as 'good practice advice' for those involved in the supply, operation and management of surveillance systems. It is there to help them comply with legislation. Information that is collected about individuals is covered by the Data Protection

Act (DPA) 1998. The guidance in the code is intended to assist organisations engaged in that activity comply with their legal obligations.

The basic legal requirement is to comply with the DPA, however organisations may also need to consider their obligations in the wider legislative environment with relation to the Freedom of Information Act (FIA) 2000, Human Rights Act (HRA) 1998 and of course the POFA.

The DPA in particular is applicable to all organisations processing personal data and the Data Protection Principles are at the heart of the recommendations contained in the Surveillance Camera Code.

General relevance to the body-worn video camera sector

Section 5 of the code is titled 'Governance'.

Much of the debate about body cameras surrounds the management of footage. The integrity of workflow is stressed throughout the industry. Establishing efficient and effective systems for processing data is essential. The code stresses that organisations should decide;

- -Who has responsibility for control of the data.
- -How the data is to be used.
- -To whom it may be disclosed.

It states “If you are the organisation that makes these decisions then you are the data controller and you are legally responsible for compliance with the Data Protection Act....Guiding Principle 5 of the POFA code emphasises the importance of clear policies and procedures and communication these to all who need to comply with them”.

-It is not required that data be captured in an encrypted format, but it is essential that the subsequent storage and workflow is considered and controlled. Encryption is certainly one method to protect data, however this can have implications for camera performance and battery life along with posing problems when evidentially relevant material must be shared along a judicial trail. SCCP;

“It is important that your information can be used by appropriate law enforcement agencies if it’s required. If it can’t, this may undermine the purpose for undertaking surveillance.”

Other methods can be employed to ensure the security of footage, as are used with any restricted data. The code suggests keeping a record or audit trail.

-There is no mandatory time limit on the retention of footage. The code simply states; “Once there is no reason to retain the recorded information, it should be deleted. Exactly when you decide to do this will depend on the purpose for using the surveillance systems.”

-Recorded images should be viewed in a restricted area, such as a designated secure office. “Viewing of live images on monitors should usually be restricted to the operator and any other authorised person where it is necessary for them to see it”.

5.2.2 Disclosure

Some common-sense guidelines are also addressed in section 5, such as the controlled disclosure of information from surveillance systems. This should be consistent with the purpose that the system was established for. In most situations it would 'not be appropriate' to place data on the internet nor 'disclose information about identifiable individuals to the media.' The use of body-worn video is lawful. Mis-use or inappropriate dissemination of footage in most cases will not be under the DPA.

5.2.3 Subject access request

It is important to note that individuals who have been recorded have the right to request access to information held about them. This is guaranteed under the Data Protection Act and must be provided promptly and in a permanent form. A fee may charged (up to 10.00 for each request) and at the discretion of the organisation other individuals identifiable in the footage may be obscured. It would be useful to take this into consideration when deciding on a retention policy.

5.2.5 Retention

“The DPA does not prescribe any specific minimum or maximum retention periods which apply to all systems or footage...It should not be kept for longer than is necessary, and should be the shortest period necessary to serve your own purpose.”

Strict control of retained data (footage) is critical for compliance, underscored by an emphasis on procedures, training and regular review of both. The code suggests the following for consideration;

- **-Have you decided on the shortest period that you need to retain the information, based upon your purpose for recording it?**
- **-Is your information retention policy documented and understood by those who operate the system?**
- **-Are measures in place to ensure the permanent deletion of information through secure methods at the end of this period?**

7.2 Body worn video (BWV)

“BWV systems are likely to be more intrusive than the more ‘normal’ CCTV style surveillance systems because of its mobility.” The key phrase for BWV is that use should be “proportionate, necessary and addresses a pressing social need.”

Key points;

- **-When to record and when not to; because BWV technology offers the ability to capture audio which is likely to be more intrusive, continuous recording will require 'strong justification.'**
- **-Informing data subjects; BWV cameras are discreet and situations may be fast-paced. Signage on camera or uniform (plus explicit articulation?) should be used to alert individuals that they are being recorded.**
- **-Workflow and retention of data (footage); you should have a controlled retention, identification and disposal policy as discussed above.**