

PROTECTION OF FREEDOMS BILL

Fact Sheet – Part 2: Regulation of Surveillance

Chapter 1: Regulation of CCTV and other surveillance camera technology

Chapter 1 meets the Government's commitment to further regulate closed circuit television (CCTV). The provisions also encompass other surveillance camera technology – in particular Automatic Number Plate Recognition (ANPR) systems.

Code of Practice

The Bill requires the Secretary of State (in practice, the Home Secretary) to produce a code of practice in relation to surveillance camera systems, including CCTV and ANPR systems. The code must include guidance on the use of such systems or the images resulting from them (for example, the retention, storage and subsequent use of such images).

The provisions enable the code to be wide-ranging with regard to the type and extent of the guidance that it includes, but do not require it to be absolutely comprehensive, nor to deal with every conceivable type of surveillance camera system (particularly those for example, which may at present be emerging or niche technologies with limited current use).

It is intended that the code of practice will be produced in consultation with those individuals or bodies most likely to have a significant interest in its operation. The legislation specifies key such bodies including the Association of Chief Police Officers; the Information Commissioner; and the new Surveillance Camera Commissioner.

From the outset, local authorities, police and crime commissioners, and police forces will be required to have regard to the code of practice. There will, however, be an incremental approach to what is necessarily a complex landscape of usage, custom and practice, and the Bill contains powers for the Home Secretary to extend this duty to have regard to the code to other operators of CCTV (or other surveillance camera) systems.

The Surveillance Camera Commissioner

This Chapter also provides for the appointment of a Surveillance Camera Commissioner. The Commissioner's responsibilities include promoting and encouraging compliance with the surveillance camera code of practice amongst users; reviewing how the code is working; and providing advice about the code (which may include, for example, advice to users of surveillance systems, members of the public, and ministers, as necessary). The Commissioner is required to report annually on the operation of the code of practice.

Chapter 2: Safeguards for certain surveillance under RIPA

Chapter 2 of Part 2 amends the Regulation of Investigatory Powers Act 2000 (“RIPA”) so that local authorities can only use covert investigatory techniques if approved by a magistrate (or, in Scotland, a sheriff).

RIPA already limits local authority authorisations to three covert techniques:

- access to some types of communications data (such as billing and subscriber information from telephone companies);
- use of directed surveillance (covert surveillance in public places); and
- use of covert human intelligence sources (CHIS) (informants and undercover officers).

These provisions deliver part of the Coalition commitment to “*ban the use of powers in RIPA by councils, unless they are signed off by a magistrate and required for stopping serious crime*”.

The serious crime threshold (offences which attract a maximum custodial sentence of 6 months or more or relate to underage sales of alcohol and tobacco) will be introduced using existing powers in RIPA and will apply to local authority use of directed surveillance only.

Authorisations requiring judicial approval

This Chapter provides that an authorisation made by a local authority will not come into effect until it has been approved by a magistrate. The magistrate will be required to consider whether it was, and continues to be, reasonable for the local authority to believe that the use of the covert technique in question is necessary and proportionate. A magistrate is able to exercise his or her own discretion and judgement when deciding whether to approve the authorisation.

Under the new arrangements, a magistrate may approve the application if satisfied that it:

- is necessary for the purposes set out in RIPA (for local authorities this is the prevention or detection of crime or prevention of disorder) and proportionate in human rights terms to what it seeks to achieve;
- has been authorised by a person in the authority at the level designated in RIPA (that is, at Director level);
- meets any other restriction imposed by order – such as the serious crime threshold that will apply to directed surveillance;
- sets out, in the case of a CHIS, that the relevant procedures and supporting officers are in place to protect the welfare and safety of the CHIS.

The measures would apply to all local authority authorisations in England and Wales and Northern Ireland and to those in respect of the acquisition and use of communications data in Scotland (local authority applications for directed

surveillance or CHIS in Scotland are subject to the Regulation of Investigatory Powers (Scotland) Act 2000).

Procedures for judicial approval

The local authority RIPA authorising officer is not required to apply in person to a magistrate.

There is no requirement to inform the subject of the investigation or their representatives.

When a magistrate refuses a local authority application he or she may quash the local authority authorisation.

**Home Office
October 2011**