Revised Codes of Practice for Covert Surveillance and Covert Human Intelligence Sources
Response from the Information Commissioner's Office

Introduction

The ICO is the UK's independent public authority set up to uphold information rights. We do this by promoting good practice, ruling on complaints, providing information to individuals and organisations and taking appropriate action where the law is broken. Our particular interest in this consultation is through our role in enforcing and overseeing the Data Protection Act 1998 throughout the UK as a whole. The focus of our comments is therefore limited to matters relating to compliance with data protection principles.

General Comments

The Regulation of Investigatory Powers (Scotland) Act 2000 (RIP(S)A) provides the regulatory framework to enable covert surveillance to be undertaken lawfully. The Codes of Practice will assist investigators to work within the parameters set by RIP(S)A and will help ensure that investigations are compliant with Article 8 of the European Convention of Human Rights. In addition, operating within the Codes will help ensure that the processing of personal data within the scope of a RIP(S)A investigation will comply with data protection principles, in particular the first, second and third data protection principles (ie, that processing is fair and lawful, the data is processed for lawful purposes and that it is adequate, relevant and not excessive). As such, the ICO welcomes the provisions of the Codes and has no substantive comments to make regarding the procedures outlined within it. However, we would wish to draw to your attention a number of points of clarification with regard to aspects of data protection referred to in the Codes.

Employment Practices Code

The first example following paragraph 2.27 of the Covert Surveillance and Property Interface Code (CSPIC) references our Employment Practices Code. It may assist readers to locate the Code by inserting a link to the ICO's website (www.ico.org.uk) as a footnote

CCTV

Paragraph 2.28 of the CSPIC notes that the use of CCTV cameras is subject to the Data Protection Act 1998 (DPA) and references our 2008 CCTV Code of Practice. We are in the process of revising this Code of Practice and expect it to be published in summer 2014. It would assist readers if this could either be noted, or the Code is updated to reference the new CCTV Code when it is published.

The Protection of Freedoms Act 2012 (PoFA) required the Secretary of State to publish a Surveillance Camera Code of Practice for England and Wales and relevant authorities specified in the PoFA must have regard to it. The Code and further information about the Surveillance Camera Commissioner can be found at www.gov.uk/government/organisations/surveillance-camera-commissioner. Whilst it does not have effect in Scotland, relevant authorities for the purpose of RIP(S)A may find the Code useful to take it into account when preparing to engage cameras for directed or intrusive surveillance.

Keeping of Records

Section 7 of the Covert Human Intelligence Sources Code (CHISC) and Section 8 of the CSPIC make reference to "specific rules relating to data retention, review and deletion under the Data Protection Act". Please note that Principle 5 of the DPA requires that "personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes" and there are no additional rules contained within the DPA. To help comply with this principle, the ICO advises that organisations should:

- review the length of time personal data is kept
- consider the purpose or purposes for which the information is held in deciding whether to retain it (bearing in mind any statutory requirements)
- securely delete information that is no longer required for these purposes
- update (where necessary), archive or securely delete information if it goes out of date.

The ICO recommends that these sections be redrafted to reflect the above.

Retention and Destruction of Material

Section 8 of the Covert Human Intelligence Sources Code (CHISC) and Section 9 of the CSPIC make reference to the need for each public authority

to ensure that arrangements are in place for the secure processing (ie, the handling, storage and destruction) of material obtained under RIP(S)A. It further states that authorising officers "must ensure compliance with the

appropriate data protection requirements under the Data Protection Act". In this regard, please note that Principle 7 of the DPA requires that "appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data".

To assist in complying with Principle 7, organisations must:

- ensure a level of security appropriate to the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage, given the nature of the data to be protected

- must take reasonable steps to ensure the reliability of any employees of his who have access to the data

- where relevant, choose a data processor providing sufficient guarantees in respect of the technical and organisational security measures governing the processing to be carried out and take reasonable steps to ensure compliance with those measures.

- where relevant, ensure that any such data processing is carried out under a contract made or evidenced in writing, obliges the data processor is to act only on instructions from the data controller and requires the data processor to comply with obligations equivalent to those imposed on a data controller by the seventh principle.

The ICO recommends that those sections be amended to reflect the above.

Dr Ken Macdonald
Assistant Commissioner (Scotland & Northern Ireland)
The Information Commissioner's Office