

Director of Legal Services :  
David Tatlow

---

# BRIEFING

## Surveillance- Regulation of Investigatory Powers Act 2000 2004 Update

---

---

### Executive Summary

1. The Regulation of Investigatory Powers Act 2000 (RIPA) governs various central and local government bodies in relation to surveillance. This is of particular importance to local authorities such as Birmingham City Council, where investigations are conducted, including in relation to benefits fraud and trading standards.
2. Failure to comply with RIPA may lead to any evidence obtained by any surveillance breaching RIPA being deemed inadmissible, and potentially lead to legal proceedings being brought against the Council, for a breach of Human Rights.
3. Furthermore, RIPA also governs in part, the usage of CCTV systems, which is dealt with in a separate briefing note.<sup>1</sup>

### Introduction

4. RIPA aims to ensure that the various investigatory powers available to public bodies are only exercised in accordance with the requirements of the Human Rights Act 1998 (HRA).
5. Part II of RIPA is concerned with covert surveillance. It sets out the purposes for which the powers may be

used, what any material obtained can be used for and who may authorise an investigation.

6. However it only provides a defence against allegations that the HRA has been breached. In certain circumstances obligations under other legislation will need to be considered.
7. RIPA came into force on 25 September 2000, and has been subsequently amended by various statutory instruments.

### Human Rights

8. Article 8 of HRA provides: -
  - i. *Everyone has the right to respect for his private and family life, his home and his correspondence.*
  - ii. *There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.*
9. The requirement in Article 8(2) that any interference be in accordance with

---

<sup>1</sup> CCTV general guidance

the law means that a legal framework must be in place to regulate the interference. The European Court of Human Rights has in the past criticised the UK for lacking an appropriate framework in the area of surveillance. RIPA is intended to remedy this.

### **Covert Surveillance**

10. RIPA is only concerned with covert surveillance. It has no application to CCTV cameras used for the general monitoring of public areas.

11. However it does apply to both human and mechanical forms of covert surveillance.

12. Section 26(9) states that surveillance is covert: -

*if and only if, it is carried out in a manner that is calculated to ensure that persons who are subject to the surveillance are unaware that it is or may be taking place.*

13. RIPA envisages three different classes of surveillance, each of which is subject to different authorisation regimes. The classes are: -

- Directed surveillance,
- Covert human intelligence source, and
- Intrusive surveillance.

### **Directed Surveillance**

14. Directed surveillance is covert surveillance undertaken in relation to a specific investigation or a specific operation which is likely to result in the obtaining of private information about a person.

15. This could include the placing of concealed CCTV cameras in a street to watch a specific suspect's activities e.g. watching them enter a certain property.

16. Directed surveillance does not include any type of covert surveillance in residential premises or in the private vehicles of the target. This is defined as "intrusive surveillance" and can not be authorised by local authority officers.

17. Authorisations for directed surveillance cannot, under Section 28, be granted unless the specific criteria in Section 28(2) are satisfied, namely, that the person granting the authorisation believes that: -

*(a) the authorisation is necessary on grounds falling within subsection (3); and*

*(b) the authorised activity is proportionate to what is sought to be achieved by it.*

18. "Proportionate" means that the nature of the surveillance exercise is reasonable in the circumstances. It equates to the maxim against "using a sledgehammer to crack a nut".

19. Prior to the changes implemented at the start of 2004, RIPA originally set out a number of specific grounds in Section 28(3) are that the authorisation is necessary: -

*(a) in the interests of national security;*

*(b) for the purpose of preventing or detecting crime or of preventing disorder;*

*(c) in the interests of the economic wellbeing of the UK;*

*(d) in the interests of public safety;*

*(e) for the purpose of protecting public health;*

*(f) for the purpose of assessing or collecting any tax, duty, levy or*

*other imposition, contribution or charge payable to a government department; or*

*(g) for the purposes which may be specified by the Secretary of State.*

20. Of these, the most common purpose utilised was (b) for the purpose of preventing or detecting crime or of preventing disorder.

21. **Due to public unease with the concept of local authorities being authorised to conduct surveillance under a wide area of grounds, RIPA was amended.** The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2003<sup>2</sup> amended RIPA **from 5 January 2004**. The primary effect of the Order was to reduce the number of grounds a local authority could utilise when authorising directed surveillance to one:

- ***for the purpose of preventing or detecting crime or preventing disorder***<sup>3</sup>

22. Many of the other grounds were transferred to other statutory bodies, i.e.(e) *for the purpose of protecting public health* was transferred to local health authorities.

### **Covert Human Intelligence Source**

23. A person is a covert human intelligence source under Section 26(8) if: -

*(a) he establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraph (b) or (c);*

*(b) he covertly uses such a relationship to obtain information or to provide access to any information to another person; or*

*(c) he covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.*

24. A covert human intelligence source would therefore include, for example, an investigating officer establishing a relationship with a person for the purposes of obtaining information relevant to an investigation without the officer revealing his or her true identity.

25. The criteria for the authorisation of the use of covert human intelligence sources set out in Section 29 are the same as with directed surveillance save that the additional criteria, in Section 29(5), must be applied. In essence they require that specific arrangements must exist to ensure that, amongst other things, the source is independently managed and supervised, that records are kept of the use made of the source and the source's identity is protected from those who do not need to know it.

26. **As in the case with directed surveillance, the amendments to RIPA reduced the grounds for covert surveillance to one sole purpose:**

- ***for the purpose of preventing or detecting crime or preventing disorder***

### **Notices requiring communications data to be obtained and disclosed**

27. Under RIPA, as amended by the Regulation of Investigatory Powers

---

<sup>2</sup> 2003 No. 3171

<sup>3</sup> s28(3)(b)

(Communications Data) Order 2003<sup>4</sup>, local authorities now have, from 5<sup>th</sup> January 2004, the power to compel communications company(s) to obtain and collect information in compliance with a notice issued by the local authority.

28. For the purposes of RIPA, a communications company is deemed to include telecommunications and postal companies.

**29. As with the other forms of surveillance that are regulated by the RIPA, a notice can only be issued for the sole purpose of preventing or detecting crime or preventing disorder.**

30. There are two types of notice:

a. where the notice authorises the local authority to collect the information directly, i.e. by allowing the local authority to fit its own equipment or place members of its own staff in the Communications Company in order to collect the information; or

b. where the notice compels the Communications Company to collect, collate and then disclose to the local authority the information sought.

31. Normally, the second option would be used, as in most situations, the Communications Company would have sufficient resources to enable it to collect the information sought by themselves.

32. This provision will tie in with the forthcoming legislation, as discussed below<sup>5</sup>.

---

<sup>4</sup> SI 2003 No. 3172

<sup>5</sup> para 42 - 48

## Authorisation

33. Under the Regulation of Investigatory Powers (Prescription of Offices, Ranks and Positions) Order 2000<sup>6</sup> the authorising officer for a local authority for the use of directed surveillance or of covert human intelligence sources is the "Assistant Chief Officer responsible for the management of an investigation". In the case of Birmingham City Council, an authorising officer is normally someone of Assistant Director level or above, who has had specific training in relation to RIPA, and is listed in the Birmingham City Council's RIPA manual as being authorised to authorise directed surveillance or covert human intelligence sources. An Authorised Officer cannot sign forms unless s/he has been certified by the Chief Legal Officer. A full copy of the Corporate Documentation on RIPA is available on Birmingham's website.

34. An authorisation may authorise more than one officer to carry out surveillance and may include a number of surveillance exercises. However it may only relate to a single investigation.

35. It is not permissible to give any officer a blanket authorisation to be relied upon in any situation.

36. Ordinarily the authorisation must be in writing. Model Authorisation documents are available on the Home Office Web Site, but versions of the forms are contained in the Birmingham City Council's RIPA Policy and Procedures Document (on the website).

37. In urgent cases authorisation may be given orally.

38. An oral authorisation lasts 72 hours. Written authorisations for the use of

---

<sup>6</sup> SI 2000.No. 2417

directed surveillance last 3 months and for the use of covert human intelligence sources last 12 months.

39. The authorisation may be renewed at any time prior to its expiry. However the same conditions apply as to the original authorisation.
40. In the case of notices seeking the obtaining and disclosing of communications data, the notice will last for a maximum of one month, but it can be renewed for further periods of one month at any time during the previous month.
41. For further guidance in respect of making applications seeking either authorisation for covert Human Intelligence Sources, Covert Surveillance or Notices requiring communications data to be obtained and disclosed, please consult the RIPA Policies and Procedures Document (on the website).

### **Future developments**

42. Following recent terrorist attacks, there is increasing emphasis being placed on surveillance and information gathering, both on a domestic level and also on a Europe-wide scale. The latest proposed legislation which, if enacted, will interact with RIPA is the Council of the European Union's draft framework decision on the retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications networks for the purposes of prevention, investigation, detection and prosecution of crime and criminal offences including terrorism<sup>7</sup> ("the Draft Decision").
43. This places a responsibility on telecommunications companies,

including Internet Service Providers and email providers, to retain details of communications made using their public telecommunications systems, for up to 3 years sufficient to allow :

- (a) the tracing and identification of a source of a communication which includes personal details, contact information and information identifying services subscribed to;
  - (b) the identification of the routing and destination of a communication;
  - (c) the identification of the time and date and duration of a communication;
  - (d) the identification of the communication;
  - (e) the identification of the communications device;
  - (f) the identification of the location at the start and throughout the duration of the communication.
44. This will, if passed, extend the effectiveness of notices requiring communications data to be obtained and disclosed by a considerable margin, and will allow the tracing of the location of individuals, usually by way of mobile telephones.
  45. Whilst similar powers have been available to the United Kingdom Government by way of the Anti Terrorism, Crime and Security Act 2001 ("ATCASA 2001"), which allows the Secretary of State to establish Codes of Practice setting out retention schedules for communications data, for the purposes of National Security. This power was subsequently utilised with the introduction of the Retention of Communications Data (Code of Practice) Order 2003<sup>8</sup>.

---

<sup>7</sup> 8958/04 dated 28 April 2004

46. The Draft Decision, if implemented, will replace ATCASA 2001, by compelling the telecommunications companies to automatically retain communications data for up to 12 months, dependent on the information retained.
47. Furthermore, it can be argued that if a notice seeking the obtaining and disclosure of communications data is made, the telecommunications company, if it is already retaining information going back, in line with code(s) of practice established under ATCASA 2001, it will be obliged to disclose the information it holds, including the retained data.
48. However, this briefing note will be updated to take account of further developments in this area as and when they occur.

#### **Further information**

49. The Home Office Web Site<sup>9</sup> which contains the legislation, guidance notes and model authorisation forms.
50. In addition, the Birmingham City Council's RIPA Policy and Procedures Manual sets out the procedure for making an application for authorisation under RIPA.

**Date: 7<sup>th</sup> September 2004**

**For advice on RIPA contact:-**

**Varun Shingari, Solicitor on: -**

**Tel: 0121 464 3459**

**Fax: 0121 303 4936**

**E-Mail: [Varun\\_Shingari@birmingham.gov.uk](mailto:Varun_Shingari@birmingham.gov.uk)**

---

<sup>9</sup> [www.homeoffice.gov.uk](http://www.homeoffice.gov.uk)