Protection of Freedoms Act 2012 – changes to provisions under the Regulation of Investigatory Powers Act 2000 (RIPA)

Home Office guidance for Magistrates' Courts in England and Wales for a local authority application seeking an order approving the grant or renewal of a RIPA authorisation or notice

Home Office

October 2012

Contents

1. INTRODUCTION

1. In the Coalition Agreement the Government gave a commitment to stop local authorities from using covert techniques authorised under the Regulation of Investigatory Powers Act 2000 ("RIPA") unless they were judicially approved and were required to stop serious crime. Local authorities have been criticised for using surveillance powers in low level cases such as dog fouling and checking that families reside within a school catchment area. The Government has committed to ensuring that local authority use of surveillance should not be allowed in low level cases.

2. This guidance is issued in response to the change in law to introduce independent judicial oversight of local authority use of RIPA. The amendments to RIPA in the Protection of Freedoms Act 2012 that take effect on 1 November 2012[1] will mean that local authority authorisations and notices under RIPA for the use of particular investigatory techniques can only be given effect once an order approving the authorisation or notice has been granted by a Justice of the Peace ("JP"). This process is not part of the local authority investigation but a statutory check on it.

3. The guidance is non-statutory and has been produced to explain the changes that are being made and to provide guidance on the legislative framework, in particular highlighting the tests that the JP must consider. This guidance is intended for Magistrates' Courts who may be required to consider an application for judicial approval by a local authority. It is supplementary to the legislation and to the statutory Codes of Practice.[2]

4. Separate guidance is available for Sheriffs in Scotland. Guidance has also been issued to local authorities.

1 Sections 37 and 38 of the Protection of Freedoms Act 2012 amend RIPA and will come into force on 1 November 2012.
2 See page 23 for links to the relevant legislation and codes of practice.

2. LOCAL AUTHORITY USE OF RIPA INVESTIGATORY TECHNIQUES

LOCAL AUTHORITY FUNCTIONS

5. Local authorities have a wide range of functions and are responsible in law for enforcing over 100 separate Acts of Parliament. In particular local authorities investigate offences in the following areas:

- Trading standards, including action taken against loan sharks and rogue traders, consumer scams, sale of counterfeit goods, unsafe toys and electrical goods.
- Environmental health, including action against large-scale waste dumping, dangerous workplaces, pest control and the sale of unfit food.
- Benefit fraud, including action to counter fraudulent claims for housing benefits, investigating 'living together' and 'working whilst in receipt of benefit' allegations and council tax evasion.

6. Local authorities are also responsible for tackling issues as diverse as anti-social behaviour, unlicensed gambling, threats to children in care, underage employment and taxi regulation.

USE OF INVESTIGATORY TECHNIQUES

7. As part of their investigation a local authority may consider that it is appropriate to use a RIPA technique to obtain evidence. In many cases this will be the only way to gather the necessary evidence.

8. The use of an investigative technique can give rise to an interference with an individual's privacy and a public authority will therefore need to consider their obligations under Article 8 of the European Convention on Human Rights (ECHR).

9. RIPA provides a legal framework for a public authority to authorise conduct which engages Article 8 ECHR. It does this by ensuring that use of the relevant techniques are authorised only if the tests of necessity, proportionality and legitimate aim are satisfied. Such a request for authorisation under RIPA is considered by designated senior officers (of a particular rank approved by Parliament) and detailed records must be kept. Independent oversight is provided by the Surveillance Commissioner, the Interception of Communications Commissioner and the Investigatory Powers Tribunal (IPT).[3] It is not the function, however, of the Commissioners to keep under review judicial decisions relating to local authority applications.[4] The IPT will continue to investigate complaints by individuals about the use of RIPA techniques by public bodies, including local authorities. If, following a complaint to them, the IPT does find fault with a RIPA authorisation or notice it has the power to quash the JP's order which approved the grant or renewal of the authorisation or notice.[5]

10. Local authorities use three investigatory techniques that can be authorised under RIPA:

- Directed surveillance
- Use of a covert human intelligence source
- Obtaining and disclosing communications data

11. RIPA does not allow the use of any other covert techniques by local authorities to be authorised. In particular, a local authority cannot be authorised under RIPA to intercept the **content** of a communication.

---

3 More information on the Investigatory Powers Tribunal can be found at www.ipt-uk.com.
4 See section 57 (4A) and section 62(2A) RIPA.
5 See section 67(7)(aa) RIPA.

DIRECTED SURVEILLANCE

12. **'Directed' surveillance** (DS) is essentially covert surveillance which is not intrusive surveillance.

13. Intrusive surveillance is surveillance carried out in relation to residential premises (including hotel bedrooms, prison cells and rented accommodation), premises where legal consultations take place or private vehicles (including hire or company cars, boats or caravans)[6]. Local authorities cannot authorise intrusive surveillance under RIPA.

14. For the purposes of RIPA, surveillance is "directed" if it is:

- covert, but not intrusive surveillance (i.e. it takes place somewhere other than residential premises, particular premises where legal consultations take place or private vehicles);
- conducted for the purposes of a specific investigation or operation e.g. pre-planned against a specific individual or group;
- likely to result in the obtaining of private information about a person; and
- conducted otherwise than as an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable to seek an authorisation under RIPA[7].

15. Surveillance is covert 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[8].

16. Further guidance on the definition of "directed surveillance" is set out in Chapter 2 of the Covert Surveillance and Property Interference Code of Practice[9].

EXAMPLE

Kent Trading Standards authorised directed surveillance to follow a rogue trader engaged in landscape gardening. The trader was known to 'cold call' vulnerable people and charge them over the odds for little work. A previous case involved him cold calling a blind elderly woman, charging her £700 to cut her very small lawn, taking her to the bank in the local town and leaving her there to find her own way home. The surveillance operation resulted in the man's arrest, the seizure of his van by the police as it was uninsured and the discovery of offensive weapons in the van.

6 Intrusive surveillance is defined in section 26(3) of RIPA. In addition, article 3 of the Regulation of Investigatory Powers (Extension of Authorisation Provisions: Legal Consultation) Order 2010 [S.I. 2010/461] provides that surveillance of legal consultations taking place in the premises listed in article 3(2) is also to be treated as intrusive surveillance.
7 See section 26(3) RIPA for the full definition.
8 See section 26(9)(a) RIPA.
9 See page 23 for links to the relevant legislation and codes of practice.

COVERT HUMAN INTELLIGENCE SOURCES

17. **Covert Human Intelligence Sources** (CHIS) include undercover officers, public informants and people who make test purchases.

18. For the purposes of RIPA[10], a person is a CHIS 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.

19. A local authority authorisation for the conduct and use of a CHIS may include:

- someone employed or engaged by a local authority to hide their true identity or motivation and covertly use a relationship to obtain information and disclose it to the local authority (an undercover officer); or
- a member of the public who provides a tip-off to a local authority and is asked to go back and obtain further information by establishing or continuing a relationship whilst hiding their true motivation (an informant).

20. Further guidance on the definition of CHIS is set out in Chapter 2 of the Covert Human Intelligence Sources Code of Practice.[11]

EXAMPLE

Norfolk County Council received reports questioning whether meat being sold by a butcher on a market stall was fit for human consumption. A joint investigation was run with the District Council Environmental Services. The source of the meat was unknown. A test purchase was carried out. Offences were revealed. The butcher was successfully prosecuted for offences relating to the failure to dispose of animal by products correctly and for food hygiene offences.

10 See section 26(8) RIPA.
11 See Section 6 for links to the relevant legislation and codes of practice.

COMMUNICATIONS DATA

21. Communications data (CD) is the 'who', 'when' and 'where' of a communication, but not the 'what' (i.e. the content of what was said or written). CD means any of the following:

- **'Traffic Data'** is information about a communication and the equipment used in transmitting it (e.g. information about the location of mobile phones, routing information such as IP address allocation)[12];
- **'Service Use Information'** is information about the use a person makes of a postal or telecommunications service (e.g. itemised telephone call records, records of connection to internet services, timing and duration of service usage)[13];
- **'Subscriber Information'** is information that communications service providers (CSPs) hold about people to whom they provide a service (e.g. names, addresses, telephone numbers)[14].

22. Further guidance on the definition of CD is set out in Chapter 2 of the Acquisition and Disclosure of Communications Data Code of Practice[15].

23. Under RIPA a local authority can only authorise the acquisition of the less intrusive types of CD: service use and subscriber information. Under no circumstances can local authorities be authorised to obtain traffic data under RIPA.

24. Local authorities are not permitted to intercept the content of any person's communications and it is an offence to do so without lawful authority.

EXAMPLE

Leicestershire County Council Trading Standards Service used CD during an investigation into car clocking. Two individuals purchased high mileage cars via vehicle auction sales and reduced their odometer readings using bespoke mileage correction equipment. Cars were subsequently sold to unsuspecting private buyers together with altered MOT certificates and falsified service histories. The criminal offences under investigation were: conspiracy to undertake a business for a fraudulent purpose, supplying goods with a false trade description and engaging in unfair commercial practice. This form of acquisitive crime allows the fraudster to make substantial financial gains whilst the purchaser is left with a vehicle of minimal resale value. This activity also harms the collective interest of businesses that operate within the retail car trade. An array of names, addresses and telephone numbers were provided by the defendants in advertisements, auction records and sales invoices. Subscriber checks acquired in relation to the telephone numbers enabled investigators to link both defendants to the purchase and sale of around forty vehicles.

12 See section 21(4)(a) and 21(6) RIPA for the full definition, and paragraphs 2.19 to 2.22 of the Acquisition and Disclosure of CD Code of Practice for further guidance and examples of traffic data.

13 See section 21(4)(b) RIPA for the full definition and paragraphs 2.23 to 2.24 of the Acquisition and Disclosure of CD Code of Practice for further guidance and examples of service use information.

14 See section 21(4)(c) RIPA for the full definition and paragraphs 2.25 to 2.29 of the Acquisition and Disclosure of CD Code of Practice for further guidance and examples of subscriber information.

15 See Section 6 for links to the relevant legislation and codes of practice.

3. GENERAL RIPA PRINCIPLES

IS A RIPA AUTHORISATION REQUIRED?

25. A local authority using investigative techniques will need to consider whether or not the use of that technique engages Article 8 of the ECHR. If it does, then obtaining an authorisation under RIPA is one way for the local authority to ensure that their activity is conducted lawfully and compatibly with the ECHR.

26. If the local authority is proposing to act covertly but Article 8 is not engaged then no RIPA authorisation is necessary. For instance, a local authority may covertly monitor traffic flows or check the volume of people using a particular facility without obtaining private information about anyone. The local authority will assess whether they should obtain authorisation under RIPA.

NECESSITY

27. A RIPA authorisation may only be granted if the authorising officer believes that the conduct is necessary for one or more of the statutory purposes. The statutory purposes in RIPA mirror the legitimate aims in Article 8(2) ECHR. The RIPA Orders[16] provide that local authorities may only authorise the use of covert techniques for the purpose of 'the prevention or detection of crime or the prevention of disorder'[17].

28. Preventing and detecting crime goes beyond the prosecution of offenders and includes actions taken to avert, end or disrupt the commission of criminal offences. The local authority must be satisfied that there is an identifiable offence to detect or prevent before authorising the use of any covert technique under RIPA.

PROPORTIONALITY

29. The authorising officer must also believe that the authorised conduct is proportionate to what is sought to be achieved. This involves balancing the seriousness of the intrusion into the privacy of the subject of the investigation (or any other person who may be affected) against the need for the activity in investigative terms. If overt investigative methods would be effective, it is unlikely to be proportionate to authorise intrusive covert activity.

16 For further information refer to: The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 (SI 2010 No. 521) and The Regulation of Investigatory Powers (Communications Data) Order 2010 (SI2010 No.480).

17 There is a further restriction on use of directed surveillance – see paragraph 55 below.

30. The authorisation will not be proportionate if it is excessive in the overall circumstances of the case. Each action authorised should bring an expected benefit to the investigation or operation and should not be disproportionate or arbitrary. The fact that a suspected offence may be serious will not alone render intrusive actions proportionate. Similarly, an offence may be so minor that any development of covert techniques would be disproportionate. The following elements of proportionality should therefore be considered:

- Balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence;
- Explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others;
- Considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result;
- Recording, as far as reasonably practicable, what other methods had been considered and why they were not implemented.

31. Particular consideration should be given to circumstances where it is likely that confidential information or matters subject to legal privilege may be acquired. This includes but is not limited to communications between a professional legal adviser and his client, a Member of Parliament and another person on constituency matters, confidential personal information, or confidential journalistic information[18].

COLLATERAL INTRUSION

32. The risk and proportionality of interfering with the privacy of people not connected with the investigation must also be weighed and, where possible, steps taken to mitigate it.

18 See Covert Surveillance and Property Interference: Code of Practice, chapter 4 and Covert Human Intelligence Sources: Code of Practice, chapter 4.

4. THE LOCAL AUTHORITY RIPA PROCESS AND THE ROLE OF THE JP

OVERVIEW OF THE PROCESS

33. The judicial approval process introduced by the Protection of Freedoms Act 2012 and coming into effect on 1 November 2012 applies to situations where a local authority applicant (i.e. the investigating officer - the person involved in conducting an investigation or operation) is intending to use a covert investigatory technique and the local authority takes the view that use of that technique should be authorised under RIPA.

34. Current practice is that the local authority will authorise internally. The applicant will complete a written RIPA authorisation or notice form setting out for consideration by the authorising officer or, for CD, the designated person; why use of a particular technique is necessary and proportionate in their investigation. This authorising officer or designated person holds a prescribed office in the relevant local authority and will consider the application, recording his/her considerations and countersign the form if he/she believes the statutory tests are met.

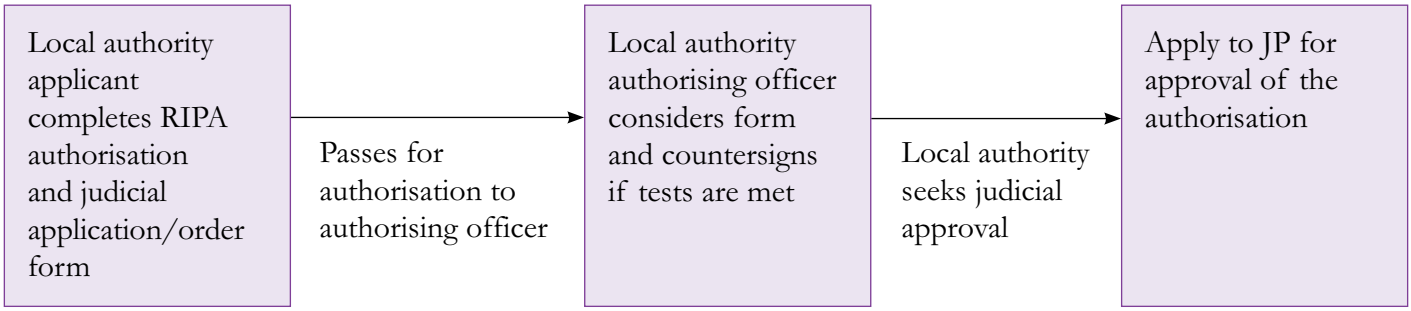
35. In the case of CD the RIPA authorisation or notice will have also been scrutinised by a single point of contact (a 'SPoC'). The SPoC is either an accredited individual or a group of accredited individuals trained to facilitate lawful acquisition of communications data and effective co-operation between a public authority and Communication Service Providers (CSPs). An accredited SPoC promotes efficiency and good practice in ensuring only practical and lawful requests for CD are made[19]. For many local authorities the SPoC services are carried out by the National Anti-Fraud Network ('NAFN') (More details on the SPoC role, NAFN and consequential acquisition of CD is contained at Annex C).

36. These practices will continue. However, there will now be an additional stage in the process for all three techniques. After the form has been countersigned the local authority will seek judicial approval for their RIPA authorisation or notice. The JP will decide whether a local authority grant or renewal of an authorisation or notice to use RIPA should be approved and it will not come into effect unless and until it is approved by a JP. Although it is possible for local authorities to request judicial approval for the use of more than one technique at the same time, in practice, as different considerations need to be applied to different techniques, this would be difficult to perform with the degree of clarity required. As a rule local authorities should aim to submit separate authorisations or notices to authorise the use of different RIPA techniques.

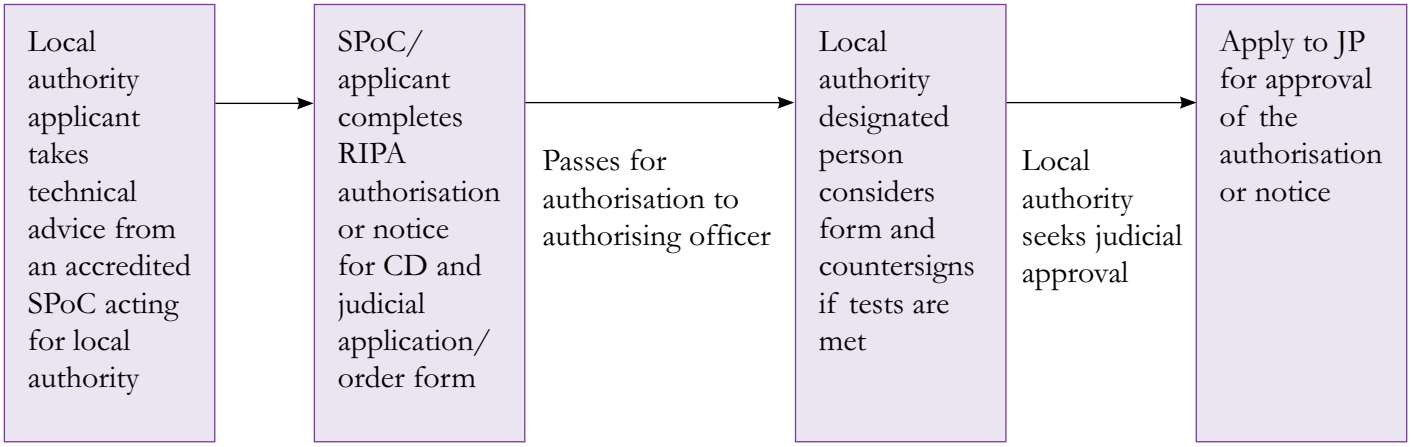
19 Acquisition and Disclosure of Communications Data: Code of Practice, paragraph 3.15

37. The process is outlined below:

DIRECTED SURVEILLANCE / CHIS (COVERT HUMAN INTELLIGENCE SOURCE)



COMMUNICATIONS DATA



THE ROLE OF THE JUSTICE OF THE PEACE

38. The role of the JP is set out in section 23A RIPA (for CD) and section 32A RIPA (for directed surveillance and CHIS).

39. These sections provide that the authorisation, or in the case of CD, the notice, shall not take effect until the JP has made an order approving such an authorisation or notice. The matters on which the JP needs to be satisfied before giving judicial approval are that:

- there were reasonable grounds for the local authority to believe that the authorisation or notice was necessary and proportionate and there remain reasonable grounds for believing that these requirements are satisfied at the time when the JP is considering the matter[20];
- in the case of a CHIS authorisation, that there were reasonable grounds for the local authority to believe that arrangements exist for the safety and welfare of the source that satisfy section 29(5) RIPA and there remain reasonable grounds for believing that these requirements are satisfied at the time when the JP is considering the matter[21];
- in the case of a CHIS authorisation, that there were reasonable grounds for the local authority to believe that the requirements imposed by Regulation of Investigatory Powers (Juveniles) Order 2000[22] were satisfied and there remain reasonable grounds for believing that these requirements are satisfied at the time when the JP is considering the matter[23];
- the local authority application has been authorised by a designated person / authorising officer.[24];
- the grant of the authorisation or in the case of CD, the notice, was not in breach of any restriction imposed by virtue of an order made under the following sections of RIPA:

  – 25(3) (for communications data),
  – 29(7)(a) (for CHIS),
  – 30(3) (for directed surveillance and CHIS)[25]:

- any other conditions that may be provided for by an order made by the Secretary of State were satisfied.

40. A detailed explanation of what is required for each of these techniques is set out in paragraphs 48 – 83 below.

41. The same considerations apply where a local authority is seeking judicial approval to continue using a technique (i.e. a renewal). Although the JP will wish to examine whether the case for a more sustained interference of Article 8 still meets the principle of proportionality. In particular he or she will want to consider the content and value of the information obtained so far.[26]

---

20 For CD see sections 23A(3) and (4) RIPA. For directed surveillance see section 32A(3) RIPA. For CHIS see section 32A(5) RIPA insofar as it relates to the requirements imposed by section 29(2)(a) and (b) RIPA.
21 See section 32A(5) RIPA insofar as it relates to the requirements imposed by section 29(2)(c) RIPA.
22 SI 2000/2793.
23 See section 32A(5) RIPA insofar as it relates to requirements imposed by virtue of section 29(7)(b) RIPA.
24 For communications data, see section 23A(5)(a)(i) RIPA. For directed surveillance, see section 32A(4)(a)(i) RIPA. For CHIS, see section 32A(6)(a)(i) RIPA. For more detailed guidance on the ranks of designated individuals see paragraphs 51-54, 67-71 and 79-82 of this guidance.
25 For communications data, see section 23A(5)(a)(ii) RIPA. For directed surveillance, see section 32A(4)(a)(ii) RIPA. For CHIS, see section 32A(6)(a)(ii) RIPA. For more detailed guidance on the restrictions imposed under the provisions referred to see paragraphs 55, 65, 66, 72, 73, and 83 below.
26 See the Covert Surveillance and Property Interference Code of Practice, Chapter 5, paragraphs 5.12-5.16, Covert Human Intelligence Sources Code of Practice, Chapter 5, paragraphs 5.17-5.22 and Acquisition and Disclosure of Communications Data Code of Practice, Chapter 3, paragraphs 3.46-3.48

DEFINITION OF A LOCAL AUTHORITY

42. RIPA defines a local authority as:

- the Common Council of the City of London in its capacity as a local authority;
- a London borough council;
- a county council or district council in England;
- a county council or county borough council in Wales; and
- the Council of the Isles of Scilly.

43. The definition of local authorities as set out in the relevant statutory instruments (Nos.480 and 521 of 2010) includes metropolitan borough councils by virtue of the Local Government Acts. There is no category of 'unitary' or 'metropolitan' or 'city' or 'borough' councils that does not fall within the definition of 'district' or 'county' council as set out in those Acts.

44. This statutory definition of a local authority does not include local authority umbrella organisations or consortia. However, a local authority can use an external contactor to carry out directed surveillance or to establish or maintain a relationship for a covert purpose. In these circumstances then that body or person must be clearly identified in the application to the JP.

TIME LIMITS

45. The current time limits for an authorisation or notice will remain.[27] That is: three months for directed surveillance and twelve months for a CHIS (one month if the CHIS is under 18). Authorisations and notices for CD will be valid for a maximum of one month from the date the JP has approved the grant. This means that the conduct authorised should have been commenced or the notice served within that month.

46. A renewal must be authorised prior to the expiry of the original authorisation, but it runs from the expiry date and time of that original authorisation. Authorisations may be renewed more than once if still considered necessary and proportionate.

47. Applications for renewals should not be made until shortly before the original authorisation period is due to expire. It is impossible to give a definitive period prior to expiry when an application for renewal should be made, but local authorities must take account of factors which may delay the renewal process (e.g. intervening weekends or the availability of the authorising officer and a JP to grant approval).

27 See section 43 RIPA

DIRECTED SURVEILLANCE

Authorisation Requiring Judicial Approval

48. Under section 28(1) RIPA, local authorities may authorise the use of directed surveillance. A local authority will need to seek judicial approval of the grant or renewal of any authorisation under RIPA.

Necessity and Proportionality

49. The requirements of necessity and proportionality are fundamental parts of the RIPA authorisation. Further guidance on these can be found in section 3 of this guidance and the relevant Code of Practice.

50. A local authority can only be authorised under RIPA to carry out directed surveillance where it:

- **is necessary for the purpose of preventing or detecting crime or of preventing disorder**[28]; and
- Meets the 'crime threshold' set out in secondary legislation which comes into effect on 1 November 2012. This is explained further in paragraph 55 of this guidance.

Authorising Officer

51. For the purposes of directed surveillance the authorising officer in a local authority is the **Director, Head of Service, Service Manager or equivalent**[29].

52. An individual holding a more senior rank may also be a authorising officer[30].

53. Where it is likely that knowledge of confidential information or matters subject to legal privilege will be acquired, the directed surveillance may only be authorised by the **Head of Paid Service**, or (in his/her absence) the person acting as the Head of Paid Service[31]. Local authorities are also subject to additional restrictions in relation to legal professional privilege, which are described further below.

54. If there is any doubt regarding sufficiency of rank the JP should request the local authority representative obtain confirmation from their Local Authority Monitoring Officer who will be able to advise them.

28 See section 28(2) and (3) RIPA which set out the necessity grounds in general. See also article 5 and the entry for local authorities (i.e. any county council, etc) in the Schedule to the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 (SI 2010/521) which limits local authorities to the necessity ground in section 28(3)(b) RIPA. Local authorities cannot authorise directed surveillance for the purpose of preventing disorder unless this involves a criminal offence which meets the threshold set out at paragraph 55.

29 See article 3(2) and the entry for local authorities (i.e. any county council, etc) in the Schedule to the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 (SI 2010/521).

30 See article 3(3) of the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 (SI 2010/521).

31 See the Covert Surveillance and Property Interference Code of Practice, Chapter 4 (particularly paragraphs 4.3 and 4.14) and Annex A.

Additional Restrictions and Conditions

Crime Threshold

55. Under the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010[32] local authorities may only authorise use of directed surveillance where they are investigating crime and where the criminal offence being investigated meets one of the following conditions:

    (a) the offence is punishable, whether on summary conviction or on indictment, by a maximum term of at least 6 months of imprisonment, or
    (b) the offence is an offence under:

        (i) sections 146, 147 or 147A of the Licensing Act 2003 or
        (ii) section 7 of the Children and Young Persons Act 1933.

Intrusive Surveillance

56. Local authorities cannot authorise the use of intrusive surveillance under RIPA.

57. Intrusive surveillance is surveillance that is carried out in relation to anything taking place on any residential premises or in any private vehicle[33]. Images taken with equipment which consistently provide the same detail or quality as if they were taken in residential premises or private vehicles constitutes 'intrusive' surveillance.

58. Additionally, surveillance of any of the following premises whilst they are being used for legal consultation is to be treated as intrusive surveillance:

    (a) any place in which persons who are serving sentences of imprisonment or detention, remanded in custody or committed in custody for trial or sentence may be detained;
    (b) any place in which persons may be detained under relevant immigration legislation;
    (c) any place in which persons may be detained under the Mental Health Act 1983;
    (d) police stations;
    (e) any place of business of any professional legal adviser;
    (f) any place used for the sittings and business of any court, tribunal, inquest or inquiry[34].

32 S.I. 2010/521, see article 7A. This restriction comes into force on 1 November 2012.
33 See section 26(3) RIPA for full definition.
34 For the definition of 'legal consultation' and the full definitions of the relevant premises, see articles 2 and 3 of the Regulation of Investigatory Powers (Extension of Authorisation Provisions: Legal Consultations) Order 2010 (SI 2010/461).

COVERT HUMAN INTELLIGENCE SOURCES

Authorisation Requiring Judicial Approval

59. Under section 29(1) RIPA, local authorities may authorise the conduct or use of a CHIS. A local authority will need to seek judicial approval of the grant or renewal of any authorisation under RIPA.

60. The local authority is not required to provide the true identity of the source either on the application form or verbally to the JP.

Necessity and Proportionality

61. The requirements of necessity and proportionality are fundamental parts of the RIPA authorisation. Further guidance on these can be found in section 3 of this guidance and the relevant Code of Practice.

62. A local authority can only be authorised under RIPA for the conduct or use of a CHIS where it **is necessary for the purpose of preventing or detecting crime or of preventing disorder.**[35]

Arrangements for the safety and security of the CHIS

63. A local authority must have arrangements in place that ensure:

- an individual in the local authority has day-to-day responsibility for dealing with the source and for the CHIS's security and welfare;
- an individual in the local authority has general oversight of the use made of the CHIS and for maintaining a record of such use;
- records relating to the CHIS contain particulars of the matters specified in the Regulation of Investigatory Powers (Source Records) Regulations 2000[36];
- records that disclose the identity of the CHIS will only be available to those who need access to them[37].

64. Where a CHIS is under the age of 16 arrangements must also include ensuring that an appropriate adult (usually a parent or carer) is present at every meeting with the local authority[38].

Restrictions on use of juveniles

65. A local authority cannot authorise the use of a CHIS under the age of 16 to gather evidence against his parents or carers[39].

35 See section 29(2) and (3) RIPA which set out the necessity grounds in general. See also article 5 and the entry for local authorities (i.e. any county council, etc) in the Schedule to the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 (SI 2010/521) which limits local authorities to the necessity ground in section 29(3)(b) RIPA.
36 SI 2000/2725 attached at Annex D.
37 See section 29(5) RIPA.
38 See article 4, Regulation of Investigatory Powers (Juveniles) Order 2000 (SI 2000/2793).
39 See article 3, Regulation of Investigatory Powers (Juveniles) Order 2000 (SI 2000/2793).

66. A local authority cannot authorise the use of a CHIS under the age of 18 without carrying out a special risk assessment in relation to any risk of physical injury or psychological distress to the source that may arise. The authorising officer must also be satisfied that any risks identified are justified and have been explained to and are understood by the CHIS. If the local authority is authorising the use of a CHIS against his parents or carers particular consideration must be given to whether this is justified[40].

Authorising Officer

67. Except as set out below, for the purposes of CHIS the authorising officer is the **Director, Head of Service, Service Manager or equivalent[41].**

68. An individual holding a more senior rank may also be a authorising officer[42].

69. Where it is likely that knowledge of confidential information or matters subject to legal privilege will be acquired, the authorising officer is the **Head of Paid Service**, or (in his/her absence) the person acting as the Head of Paid Service[43]. Local authorities are also subject to additional restrictions in relation to legal professional privilege, which are described further below.

70. Where the CHIS is a juvenile or a vulnerable individual the authorising officer is the **Head of Paid Service** or (in his/her absence) the person acting as the Head of Paid Service[44].

71. If there is any doubt regarding sufficiency of rank the JP should request the local authority representative obtain confirmation from their Local Authority Monitoring Officer who will be able to advise them.

Additional Restrictions and Conditions

Vulnerable Individuals

72. A vulnerable individual is a person who is or may be in need of community care services by reason of mental or other disability, age or illness and who is or may be unable to take care of himself or unable to protect himself against significant harm or exploitation. A vulnerable individual should only by authorised to act as a CHIS in the most exceptional circumstances[45].

Matters subject to Legal Privilege

73. Where the activities of a CHIS will result in the CHIS obtaining, providing access to or disclosing matters subject to legal privilege, a local authority must obtain prior approval from the Surveillance Commissioners before authorising such conduct[46]. The local authority should provide the JP with copies of any such approval as part of their application process.

---

40 See article 5, Regulation of Investigatory Powers (Juveniles) Order 2000 (SI 2000/2793).
41 See article 3(2) and the entry for local authorities (i.e. any county council, etc) in the Schedule to the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 (SI 2010/521).
42 See article 3(3) of the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 (SI 2010/521).
43 See Annex A of both the Covert Human Intelligence Sources Code of Practice and the Covert Surveillance and Property Interference Code of Practice.
44 See paragraphs 4.22 and 4.23 of the Covert Human Intelligence Sources Code of Practice.
45 See paragraph 4.22 of the Covert Human Intelligence Sources Code of Practice.
46 See Parts 2 and 3 of the Regulation of Investigatory Powers (Covert Human Intelligence Sources: Matters Subject to Legal Privilege) Order 2010 (SI 200/123)

COMMUNICATIONS DATA

Authorisation Requiring Judicial Approval

74. A local authority will need to seek judicial approval of the grant or renewal of an "authorisation" or of the giving or renewal of a "notice" under RIPA.

75. Under section 22(3) RIPA, local authorities may authorise the acquisition of CD by an 'authorisation'. An authorisation will be used where the designated person is authorising a person working in the same public authority to engage in specific conduct. This will normally be the public authority's SPoC. Under section 22(4) RIPA, local authorities may serve a 'notice' on a CSP to obtain and disclose the data themselves[47].

76. The authorisation or notice under RIPA may only relate to Service Use Information or Subscriber Information (see paragraph 21-24 of this guidance). CD requests may seek to acquire consequential acquisition of specific subscriber information. The necessity and proportionality of acquiring consequential acquisition will be assessed by the JP as part of his consideration (see Annex C for considerations relating to CD authorisations and notices).

Necessity and Proportionality

77. The requirements of necessity and proportionality are fundamental parts of the RIPA authorisation. Further guidance on these can be found in section 3 of this guidance and the relevant Codes of Practice.

78. A local authority can only be authorised under RIPA to obtain CD where it is necessary **is necessary for the purpose of preventing or detecting crime or of preventing disorder[48].**

Authorising officer / Designated Person

79. For the purposes of CD the authorising officer / designated person is the **Director, Head of Service, Service Manager or equivalent[49].**

80. An individual holding a more senior rank may also be an authorising officer / designated person[50].

81. The authorising officer's counter signature will in all cases show the rank or title of the grade and cover a clear description in his or her own words of what is being authorised and against which subjects or location ('who, what, where, when and how'). For many CD requests the forms are completed electronically, including the insertion of an electronic signature for the designated person.

47 For further guidance see paragraphs 3. 23 to 3.41 of the Acquisition and Disclosure of Communications Data Code of Practice.

48 See section 22(1) and (2) RIPA which set out the necessity grounds in general. See also article 3(3) and the entry for local authorities (i.e. the Common Council of the City of London, etc) in Schedule 2, Part 2 of the Regulation of Investigatory Powers (Communication Data) Order 2010 (SI 2010/480) which limits local authorities to the necessity ground in section 22(2)(b) RIPA.

49 See article 4(1) and the entry for local authorities (i.e. the Common Council of the City of London, etc) in Schedule 2, Part 2 of the Regulation of Investigatory Powers (Communication Data) Order 2010 (SI 2010/480).

50 See article 4(2) of the Regulation of Investigatory Powers (Communication Data) Order 2010 (SI 2010/480).

82. If there is any doubt regarding sufficiency of rank the JP should request the local authority representative obtain confirmation from their Local Authority Monitoring Officer who will be able to advise them.

Additional Restrictions and Conditions

83. Local authorities may only acquire service use information or subscriber information. They may not acquire traffic data[51].

51 See article 6(4) and the entry for local authorities (i.e. the Common Council of the City of London, etc) in Schedule 2, Part 2 of the Regulation of Investigatory Powers (Communication Data) Order 2010 (SI 2010/480).

5. PROCEDURE AND DECISION

84. A flowchart at Annex A details each stage of this process from receipt of the local authority application to the decision made by the JP.

RELEVANT MAGISTRATES' COURTS RULES

85. The procedures and practice governing the JP's role in examining and deciding on local authority applications for the use of the techniques regulated by RIPA are covered in England and Wales by court rules.[52] The Rules set out that the hearing will not be in open court, and no press, public, the subject of the investigation or the subject's legal representative will be present. In order to maintain privacy, notice of the application is not required to the person whom the authorisation or notice concerns or that person's legal representatives.

86. The form and supporting papers must by themselves make the case. It is not sufficient for the local authority to provide oral evidence where this is not reflected or supported by the form and papers. However, the JP may wish to note on the form any additional information he or she has received during the course of the hearing rather than requiring the application to be re-submitted. Information fundamental to the case must not be submitted in this manner.

URGENT CASES

87. No RIPA authority is required in immediate response to events or situations where it is not reasonably practicable to obtain it (for instance when criminal activity is observed during routine duties and officers conceal themselves to observe what is happening).

88. On the rare occasions where out of hours access to a JP is required then it will be for the local authority to make local arrangements with the relevant HM Courts and Tribunals Service (HMCTS) legal staff. In these cases the local authority will need to provide two partially completed judicial application/order forms so that one can be retained by the JP. The local authority will provide a copy of the signed application/order form to the court the next working day in the same way as applications for other urgent matters.

FORMS

89. The local authority will provide the JP with a copy of the original RIPA authorisation or notice and the supporting documents setting out the case.[53] This forms the basis of the authorisation and should contain all information that is relied upon.

90. Local authorities may use the RIPA forms available on the Home Office website[54]. These simply summarise the information that RIPA requires in order to generate a properly considered authorisation for each technique.

52 See Part 6 of the Criminal Procedure Rules.
53 No fee is payable for these applications as they are criminal proceedings.
54 www.homeoffice.gov.uk/counter-terrorism/regulation-investigatory-powers/ripa-forms

91. There is no requirement in law to use the Home Office forms, but applications must contain all the relevant information. Some local authorities adapt the Home Office forms, for example to incorporate logos or to reflect local procedures or processes.

92. The original RIPA form should be shown to the JP but will be retained by the local authority so that it is available for inspection by the Commissioners' offices and in the event of any legal challenge or investigations by the Investigatory Powers Tribunal. The court must take a copy of the RIPA authorisation / notice. JPs must ensure they have copies of all documentation for storage by HMCTS in compliance with Rule 5 of the Criminal Procedure Rules, and in order to deal with queries and complaints.

93. In addition, the local authority will provide the JP with a partially completed judicial application/order form (at Annex B). The local authority should complete their section of the form before the hearing.

94. This form will be the official record of the JP's decision. However, although the local authority is required to provide a brief summary of the circumstances of the case on the judicial application form, this is supplementary to and does not replace the need to supply the original RIPA authorisation or notice as well.

LOCAL AUTHORITY REPRESENTATION

95. Local authorities will choose the most appropriate representatives to present their RIPA application to the JP. It is expected that most authorities will designate investigative officers under section 223 of the Local Government Act 1972 to appear on their behalf, rather than a solicitor. This is because the local authority investigator knows the most about the investigation and will have determined that use of a covert technique is required in order to progress a particular case. The investigator will make the case on the RIPA authorisation or notice so that the authorising officer or designated person can consider the tests of necessity and proportionality. This does not, however, remove or reduce in any way the duty on the authorising officer to determine whether the tests are met.

96. For CD applications, the local authority may consider it appropriate for the SPoC (single point of contact for CD RIPA authorisations) to attend (see Annex C). Designation under section 223 of the Local Government Act 1972 by way of the local authority Standing Orders will enable investigation staff or SPoCs to attend for this purpose. It is not envisaged that the skills of legally trained personnel will be required to make the case and this would be likely to, unnecessarily, increase the costs of local authority applications.

DECISION

97. The JP should record his/her decision on the order section of the judicial application/order form. The JP will sign, date and endorse the time of decision. A copy will be provided to the local authority.

98. The JP may decide to[55] –

- **Approve the grant or renewal of an authorisation or notic**e

  The grant or renewal of the RIPA authorisation or notice will then take effect and the local authority may proceed to use the technique in that particular case.

  In relation to CD, the local authority will be responsible for providing a copy of the order to the SPoC .

- **Refuse to approve the grant or renewal of an authorisation or notice**

  The RIPA authorisation or notice will not take effect and the local authority may not use the covert technique.

  Where an application has been refused the local authority may wish to consider the reasons for that refusal. For example, a technical error in the form may be remedied without the local authority going through the internal authorisation process again. The local authority may then wish to reapply for judicial approval once those steps have been taken.

- **Refuse to approve the grant or renewal and quash the authorisation or notice**

  This applies where a magistrates' court refuses to approve the grant, giving or renewal of an authorisation or notice and decides to quash the original authorisation or notice.

  The court must not exercise its power to quash that authorisation or notice unless the applicant has had at least 2 business days from the date of the refusal in which to make representations.[56]

55 See sections 23B(3) and 32B(3) RIPA.
56 See the amended Rule 6 of the Criminal Procedure Rules.

6. OTHER SOURCES OF REFERENCE

- The Regulation of Investigatory Powers Act 2000
  http://www.legislation.gov.uk/ukpga/2000/23/contents

- RIPA Explanatory Notes
  http://www.legislation.gov.uk/ukpga/2000/23/notes/contents

- RIPA statutory codes of practice

  Covert Surveillance and Property Interference
  http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa/forms/code-of-practice-covert

  Covert Human Intelligence Sources
  http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa/forms/code-of-practice-human-intel

  Acquisition & Disclosure of Communications Data
  http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa/forms/code-of-practice-acquisition

- SI 2000 No.2793 (The Regulation of Investigatory Powers (Juveniles) Order 2000
  http://www.legislation.gov.uk/uksi/2000/2793/made

- SI 2010 No.480 - Regulation of Investigatory Powers (Communications Data) Order 2010
  http://www.legislation.gov.uk/uksi/2010/480/contents

- SI 2010 N0.521 - Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010
  http://www.legislation.gov.uk/uksi/2010/9780111490365/contents

- SI 2010 No.461 (The Regulation of Investigatory Powers (Extension of Authorisation Provisions: Legal Consultations) Order 2010
  http://www.legislation.gov.uk/uksi/2010/461/contents

- SI 2012 No.1500 (The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012)
  http://www.legislation.gov.uk/uksi/1500/contents

7. HOME OFFICE POINT OF CONTACT

Further information is available on request from:

RIPA Team
Home Office
5th Floor Peel Building
2 Marsham Street
London SW1P 4DF
Email: commsdata@homeoffice.x.gsi.gov.uk

ANNEX A

PROCEDURE: LOCAL AUTHORITY APPLICATION TO A JUSTICE OF THE PEACE SEEKING AN ORDER TO APPROVE THE GRANT OF A RIPA AUTHORISATION OR NOTICE

IN COURT HOURS

The local authority will contact Her Majesty's Courts and Tribunals Service (HMCTS) administration, who will schedule a hearing.

Local authority representative will attend the hearing with the original:

- counter-signed RIPA authorisation or notice form;
- the accompanying judicial application/order and;
- any other relevant reference material.

JP ensures that sufficient privacy is given to the hearing commensurate with the covert nature of the investigation (ie. no press, public, subject or legal representative present or court staff apart from Legal Adviser).

JP will consider papers presented by local authority, asking any additional questions in order to conclude whether an order to approve the grant of a RIPA authorisation or notice should be made. The papers by themselves make the case. It is not sufficient for the JP to rely solely on oral evidence where this is not reflected or supported by the form/papers.

OUT OF COURT HOURS

A JP may consider an authorisation out of hours, in exceptional circumstances:

- The local authority will call the court out of hours HMCTS legal staff who will ask for the basic facts and assess the urgency of the authorisation/notice. If the police are involved in the authorisation, the local authority will need to address why they cannot make the RIPA authorisation;
- If urgency is agreed, then HMCTS will arrange for local authority to attend a suitable location;
- Two copies of the forms and supporting material should be available so that one set can be retained by the JP.

The JP must be satisfied that:

- there were 'reasonable grounds' for the local authority to believe the authorisation or renewal was both 'necessary' and 'proportionate', including whether all reasonable alternatives have been considered;
- the reasonable grounds as articulated by the local authority continue to apply and the authorisation/notice continues to be necessary and proportionate;
- the local authority authorisation has been authorised by an appropriate designated person;
- there is no breach of any other restrictions imposed by order, see paragraphs 55-58, 72-73 and 83 of this guidance.

Refuse to approve the grant or renewal and quash the authorisation or notice.	Refuse to approve the grant or renewal of the authorisation or notice.	Approve the grant or renewal of the authorisation or notice.
The court must not exercise its power to quash an authorisation or notice unless the applicant has had at least 2 business days from the date of the refusal in which to make representations.	The grant or renewal of the RIPA authorisation or notice will not take effect and the local authority may not use the covert technique. Local authority may reapply addressing for example, a technical error.	Technique may be used. Local authority to resubmit any renewal or authorisation for the use of a different technique in this case.

Provide local authority representative with a copy of the signed order and return original RIPA form and any papers.
Legal Adviser or JP delivers copy order and authorisation to court admin office. Orders are kept securely and retained for 6 years.
Complete court hardcopy court log [do NOT enter details on LIBRA].
Court maintains a copy of the court order and will send a yearly return to MOJ.

ANNEX B

Application for judicial approval for authorisation to obtain or disclose communications data, to use a covert human intelligence source or to conduct directed surveillance. Regulation of Investigatory Powers Act 2000 sections 23A, 23B, 32A, 32B.

Local authority:.....

Local authority department:.....

Offence under investigation:.....

Address of premises or identity of subject:.....

.....

.....

Covert technique requested: (tick one and specify details)

Communications Data ☐

Covert Human Intelligence Source ☐

Directed Surveillance ☐

Summary of details

.....

.....

.....

.....

.....

.....

Note: this application should be read in conjunction with the attached RIPA authorisation/RIPA application or notice.

Investigating Officer:.....

Authorising Officer/Designated Person:.....

Officer(s) appearing before JP:.....

Address of applicant department:.....

.....

Contact telephone number:.....

Contact email address (optional):.....

Local authority reference:.....

Number of pages:.....

Order made on an application for judicial approval for authorisation to obtain or disclose communications data, to use a covert human intelligence source or to conduct directed surveillance. Regulation of Investigatory Powers Act 2000 sections 23A, 23B, 32A, 32B.

Magistrates' court: .....

Having considered the application, I (tick one):

☐ am satisfied that there are reasonable grounds for believing that the requirements of the Act were satisfied and remain satisfied, and that the relevant conditions are satisfied and I therefore approve the grant or renewal of the authorisation/notice.

☐ refuse to approve the grant or renewal of the authorisation/notice.

☐ refuse to approve the grant or renewal and quash the authorisation/notice.

Notes

.....

.....

.....

.....

.....

Reasons

.....

.....

.....

.....

.....

.....

Signed:

Date:

Time:

Full name:

Address of magistrates' court:

ANNEX C

COMMUNICATIONS DATA RIPA AUTHORISATIONS OR NOTICES

Single Point of Contact (SPoC)

1. For CD requests, a Single Point of Contact (SPoC) undertakes the practical facilitation with the communications service provider (CSP) in order to obtain the CD requested. They will have received training specifically to facilitate lawful acquisition of CD and effective co-operation between the local authority and communications service providers.

2. Local authorities unable to call upon the services of an accredited SPoC should not undertake the acquisition of CD.

3. For CD requests the Home Office envisages that the local authority may also choose to authorise, under Section 223 of the Local Government Act, their SPoC in order that they may appear in front of the JP if required. In cases where the type of CD or its retrieval is technically complex and the JP wants to satisfy him/herself that the CD sought meets the test, then the SPoC may be best placed to explain the technical aspects.

The National Anti Fraud Network (NAFN)

4. The National Anti-Fraud Network provides a SPoC service to local authorities, preventing each authority from the requirement to maintain their own trained staff and allowing NAFN to act as a source of expertise. Local authorities using the NAFN SPoC service will still be responsible for submitting any applications and a designated person in the local authority is still required to scrutinise and approve any applications. The accredited SPoCs at NAFN will examine the applications independently and provide advice to applicants and designated persons to ensure the local authority acts in an informed and lawful manner.

5. The local authority investigator (i.e. the applicant) will then submit the relevant judicial application/order form, the RIPA authorisation or notice and any supporting material to the JP. As above, following a private hearing, the JP will complete an order reflecting their decision. The local authority investigator will then upload a copy of this order to the NAFN SPoC.

6. The NAFN SPoC will then acquire the CD on behalf of the local authority in an efficient and effective manner.

Consequential Acquisition

7. Section 3.31 of the Code of Practice for the Acquisition and Disclosure of CD outlines that a designated person may, at the time of granting an authorisation or notice for service usage data, also authorise the consequential acquisition of specific subscriber information. The designated person may only do so to the extent where it is necessary and proportionate. The consequential acquisition may only be for subscriber data, not traffic data, which local authorities may not acquire nor service usage data. Where a SPoC has been authorised to engage in conduct to obtain details of a person to whom a service has been provided and concludes that data is held by a CSP from which it cannot be acquired directly, the SPoC may provide the CSP with details of the authorisation granted by the designated person in order to seek disclosure of the required data[57].

8. In cases where an authorisation or notice seeks to acquire consequential acquisition of specific subscriber information the JP will assess this as part of his/her consideration. The local authority investigator should be prepared to explain to the JP the reasoning behind the request for consequential acquisition and be able to show how it meets the necessity and proportionality tests.

9. In cases where consequential acquisition is approved, but where a notice is required (which must specify the name of the CSP to whom it is given, and be signed by the designated person), a further grant of a notice will be required. This is a new legal instrument and therefore will require a further visit to the designated person and the JP, despite authority for the human rights interference having already been given.

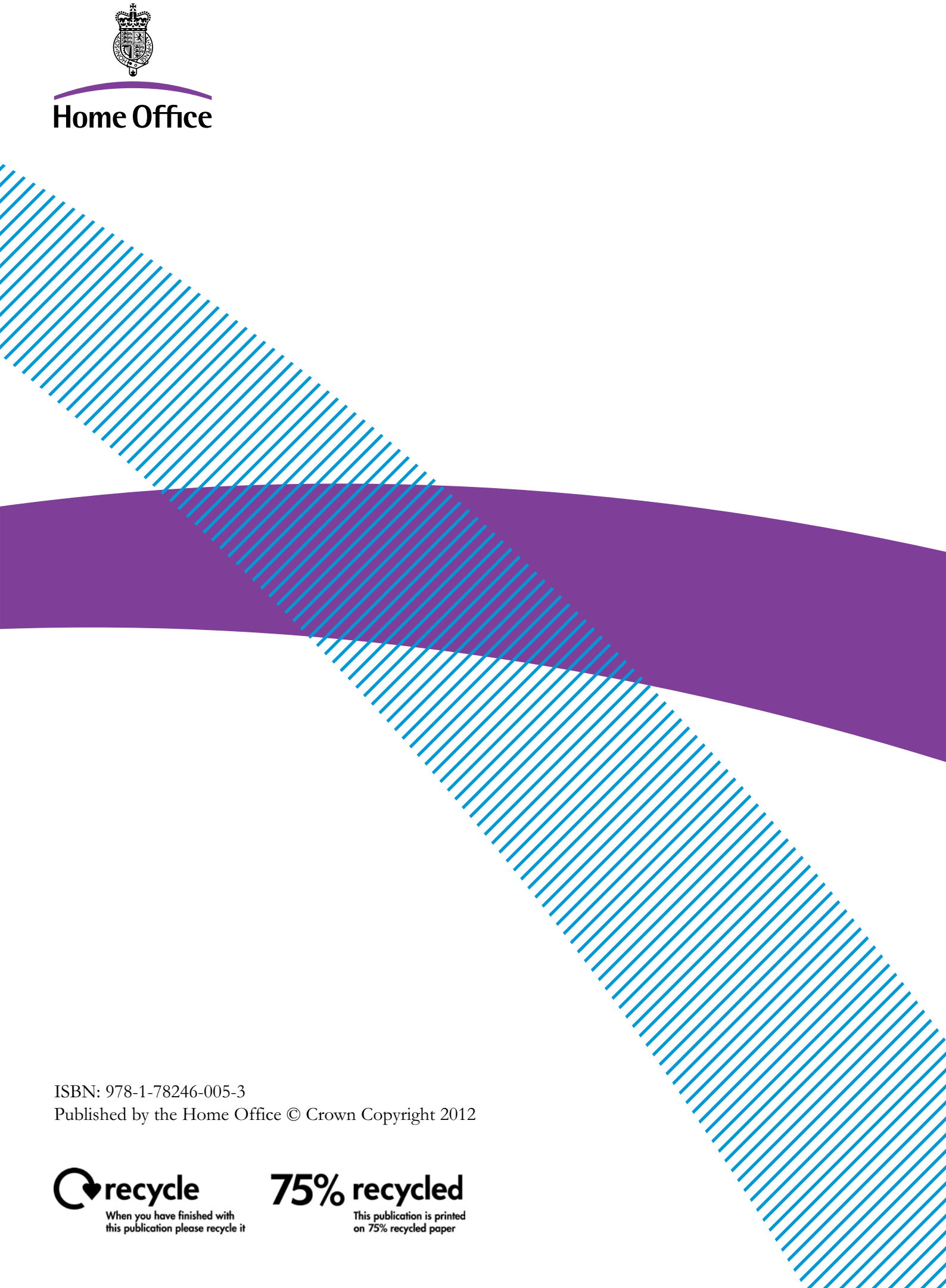
57 Acquisition and Disclosure of Communications Data Code of Practice, Paragraph 3.30.

ANNEX D

REGULATION OF INVESTIGATORY POWERS (SOURCE RECORDS) REGULATIONS 2000

The following matters are specified for the purposes of paragraph (d) of section 29(5) of the 2000 Act (as being matters particulars of which must be included in the records relating to each source):

(a) the identity of the source;
(b) the identity, where known, used by the source;
(c) any relevant investigating authority other than the authority maintaining the records;
(d) the means by which the source is referred to within each relevant investigating authority;
(e) any other significant information connected with the security and welfare of the source;
(f) any confirmation made by a person granting or renewing an authorisation for the conduct or use of a source that the information in paragraph (d) has been considered and that any identified risks to the security and welfare of the source have where appropriate been properly explained to and understood by the source;
(g) the date when, and the circumstances in which, the source was recruited;
(h) the identities of the persons who, in relation to the source, are discharging or have discharged the functions mentioned in section 29(5)(a) to (c) of the 2000 Act or in any order made by the Secretary of State under section 29(2)(c);
(i) the periods during which those persons have discharged those responsibilities;
(j) the tasks given to the source and the demands made of him in relation to his activities as a source;
(k) all contacts or communications between the source and a person acting on behalf of any relevant investigating authority;
(l) the information obtained by each relevant investigating authority by the conduct or use of the source;
(m) any dissemination by that authority of information obtained in that way; and
(n) in the case of a source who is not an undercover operative, every payment, benefit or reward and every offer of a payment, benefit or reward that is made or provided by or on behalf of any relevant investigating authority in respect of the source's activities for the benefit of that or any other relevant investigating authority.



ISBN: 978-1-78246-005-3