LIBERTY

PROTECTING CIVIL LIBERTIES
PROMOTING HUMAN RIGHTS

SUMMARY OF SURVEILLANCE POWERS UNDER RIPA[1]

There are five types of surveillance regulated by the *Regulation of Investigatory Powers Act 2000* (RIPA):

1. Interception of Communications –this is usually intercepting a person's telephone or accessing the content of a person's private emails or correspondence. In 2009 the Home Secretary issued 1514 interception warrants.[2]

2. Intrusive Surveillance – covert surveillance in residential premises or in private vehicles – so covertly filming a person's house, bugging a house or car. It is not intrusive if a device simply tells you about the location of a vehicle. Also not intrusive if a surveillance device is not physically present in premises/car - unless it *consistently* provides info of the *same quality and detail* as one present would. (s 26(5)). Note, if the surveillance involves entry onto private premises (i.e. to place the bug, which includes entry into office premises) or interference with wireless telegraphy, this is dealt with in respect of police under Part 3 of the *Police Act 1997* (1997 Act), and in respect of intelligence services, under section 5 of the *Intelligence Services Act 1994*. In 2009-2010 there were 384 intrusive surveillance authorisations under RIPA

[1] Please note that this is intended as a summary only of RIPA. It does not consider all aspects of RIPA (in particular it does not consider Part III on encryption). This summary (updated August 2010) should not be relied on in place of an up-to-date version of the Act.
[2] See *Report of the Interception of Communications Commissioner for 2009*, by the Rt Hon Sir Paul Kennedy, printed 27 July 2010, para 2.29, available at: http://www.official-documents.gov.uk/document/hc1011/hc03/0341/0341.pdf

and 2,705 property interference authorisations under the 1997 Act.[3] The number of warrants issued to the security services is not made public.[4]

3. Directed Surveillance – covert surveillance mainly in a public place – so covertly monitoring the movements and actions of specific targets, following them around, listening in or filming in mainly public spaces. It is directed if it is for a specific investigation/operation in a manner likely to obtain private information about a person – which includes any information relating to a person's private or family life (s 26(2) and (10)). In 2009-2010 law enforcement agencies obtained 15,285 directed surveillance authorisations, and other public authorities obtained 8,477 authorisations.[5]

4. Covert Human Intelligence Sources –A CHIS is a person who, under direction from a public authority, establishes or maintains a personal or other relationship in order to (covertly) use the relationship to obtain information or disclose information gained from the relationship. This includes undercover agents and informants. This power is available to numerous public authorities including local authorities. In 2008-2009 there were 5,320 CHIS recruited by law enforcement agencies and all other public authorities recruited 229 CHIS.[6]

5. Communications Data – this contains the record of a communication, such as a telephone call, email or website visited – it does not contain the content of the communication. There are three types of data covered by this:
    (a) Traffic data: this tells you where the mobile phone, internet connection etc was located at the time the communication took place – e.g. where a mobile phone was when it received or made a call;

---

[3] See the *Annual Report of the Chief Surveillance Commissioner to the Prime Minister and to Scottish Ministers for 2009-2010*, by the Rt Hon Sir Christopher Rose, printed 27 July 2010, at paras 4.3 and 4.4, available at: http://www.official-documents.gov.uk/document/hc1011/hc01/0168/0168.pdf

[4] Report of the Intelligence Services Commissioner for 2008, The Rt Hon Sir Peter Gibson, printed 21 July 2009, see para 35 where the Commissioner states "*I do not propose to disclose publicly the numbers of warrants or authorisations issued to the security and intelligence agencies*", available at: http://www.official-documents.gov.uk/document/hc0809/hc09/0902/0902.pdf

[5] See above note 2, *Annual Report of the Chief Surveillance Commissioner,* at para 4.7.

[6] Ibid at para 4.8.

(b) Service use: this tells you how a communication occurred (i.e. was it via email, a text or a phone call etc), the date and time it occurred and how long it lasted;

(c) Subscriber information: this tells you any information held by the person who has signed up to the communications service, for example the name and address and any direct debit details of the user.

During the year ended 2008 public authorities as a whole made 525,130 requests for communications data, with 1,756 requests made by local authorities.[7]

(s 48) Definition of 'surveillance' includes monitoring, observing or listening to persons, their movements, their conversations or their other activities or communications, recording any of this. This includes surveillance with the assistance of a surveillance device. It doesn't included reference to conduct by a CHIS or entry on premises or interference with property or wireless telegraphy as authorised under the ISA 1994 or Police Act 1997.

References to surveillance only includes references to interception IF one of the people sending or receiving the communication has consented to it being intercepted and there is no interception warrant authorising it.

Compliance

- It is an offence to intercept post/ public telecommunications within the UK unless it is authorised under RIPA or another statute (or have consent). (s 1)
- Failure of a postal or telecommunications operator to comply with a notice authorising acquisition of comms data is a duty enforceable by civil proceedings (22(6) and (8))
- A public authority that carries out intrusive or directed surveillance or uses CHIS without obtaining authorisation under RIPA will not be in breach of RIPA. At most it might be in breach of s 6 of the Human Rights Act 1998, or evidence might be excluded by the court.

[7] See above note 1, *Report of the Interception of Communications Commissioner*, at paras 3.8 and 3.41.

Interception of Communications

Method of authorisation

The Secretary of State must issue a warrant to intercept communications.

Reason for Authorisation

A warrant can be issued if it would be proportionate to do so and necessary for: (s 5)

- National security
- Prevent/detect *serious* crime
- To safeguard the economic well-being of the UK
- To give effect to an international mutual assistance agreement (dealing with serious crime).

Who has access?

An application for a warrant can be made by the heads of:

- the Security Service (MI5)
- the Secret Intelligence Service (MI5)
- GCHQ
- SOCA
- Police forces
- Competent authorities of overseas country re International Mutual Assistance Agreements. (s 6 RIPA).

Existence of warrant must be kept secret (it is an offence not to) (s 19)

Intrusive Surveillance

Method of authorisation

(Note below re policing and intelligence services – entry onto premises to bug dealt with under separate Acts)

On application by the intelligence services, Ministry of Defence, armed forces – Secretary of State must grant authorisation by a warrant (s 41 and 42). Warrant lasts 6 months (s 44), can be renewed at any time.

On application by police, SOCA, HMRC and OFT (s 32):

- Non urgent cases:
    - Initially authorised by senior official in that organisation, which must be in writing;
    - Authorisation only becomes effective once approved by a Surveillance Commissioner (Commissioners must hold or have held high judicial office);
    - Lasts 3 months (can be renewed at any time)
- Urgent cases:
    - If urgent and not reasonably practicable to have senior person authorise it, then a person with a lesser rank can give authorisation (s 34 RIPA). Can be given orally
    - Comes into effect on authorisation (without need for approval by Surveillance Commissioner) (s 36)
    - Lasts 72 hours (s 43)

Reason for Authorisation

Can get authorisation if it would be proportionate to do so and necessary for (s 32):

- National security
- Prevent/detect *serious* crime
- In the interests of the economic well-being of the UK

Who has access?

With Secretary of State warrant (s 42):

- the intelligence services (MI5, MI6 and GCHQ)
- an official of the Ministry of Defence
- a member of Her Majesty's forces
- a member of a designated authority – so far those designated are:
    - all offices, ranks and positions in Her Majesty's Prison Service in the Ministry of Justice (see SI 2001/1126); and
    - a person holding an office, rank or position in the Northern Ireland Prison Service (see SI 2003/3174).

With Surveillance Commissioner oversight (s 32):

- All police forces
- Service police (such as Military of Defence, Navy, Air Force and Transport Police)
- SOCA
- HMRC
- OFT

Entry onto private premises (to place the surveillance device)

If surveillance involves covert entry onto private premises or interference with wireless telegraphy, this must be authorised, not under RIPA (see s 48(3)(c) of RIPA), but:

- in the case of the intelligence services, under s 5 of the *Intelligence Services Act 1994*
- in all other cases, under Part III of the *Police Act 1997*

Intelligence services – s 5 of ISA

Secretary of State issues warrant to MI5, MI6 or GCHQ. But if entry onto premises is in a prison, it is dealt with under the prison rules, and if it is in a psychiatric hospital it is dealt with under those rules. Warrant lasts 6 months.

Police Act 1997 entry

This is the main route by which policing bodies will obtain authorisation for interfering with property (eg to place devices).

Method of authorisation:

Can be authorised by:

- Chief Constable of police or assistant chiefs
- Military Police
- IPCC
- SOCA
- OFT
- HMRC

If not urgent then authorisation last 3 months (s 92 Police Act).
If urgent, authorisation is for 72 hours.

Entry will also need the approval of a Surveillance Commissioner (unless urgent) if (s 97):

- the property is a dwelling or a hotel bedroom; or
- the property is office premises; or
- information acquired is likely to be legally privileged, confidential personal information or confidential journalistic information.

Reason for authorisation

Can be authorised if necessary to prevent/detect serious crime and it's proportionate.
'Serious' means:

- involves the use of violence, or
- results in substantial financial gain; or
- involves a large number of people acting in a common purpose; or
- is an offence for which you could be sentenced to three or more years imprisonment

In Northern Ireland – this includes national security.
If it's the OFT – only applies to cartel offences

Directed Surveillance

Method of authorisation

Self-authorised: Authorised by 'designated person' in that organisation (s 28) and the ranks or office of who is able to authorise directed surveillance is as prescribed (s 30).

But no authorisation needed for an immediate response to events or circumstances the nature of which it would not be reasonably practicable for an authorisation to be sought (s 26(2))

Reason for Authorisation

Can get authorisation if it would be proportionate to do so and necessary for (s 28(3)):

a. National security
b. Prevent/detect crime or prevent disorder
c. In the interests of the economic well-being of the UK
d. Interests of public safety
e. Protect public health
f. Collect taxes, duty etc
g. For anything else specified in an order (none specified to date for directed surveillance.

Who has access?

Schedule 1, Parts 1 and 2 of RIPA sets out who has access (can be amended by order). Includes a vast range of bodies including the police, SOCA, intelligence services, HMRC, government departments, all local authorities, fire authorities, Charity Commission, Environment Agency, Financial Services Authority, Food Standards Agency, Gambling Commission, Office of Fair Trading, Gangmasters Licensing Authority, Care Quality Commission, AND Health and Safety Executive, NHS bodies, Inspector of Education, Information Commissioner, Royal Pharmaceutical Society etc.

NOTE- the purposes that organisations can use this type of surveillance depends on the particular organisation. So, for example, police forces can use this surveillance for all of the purposes listed in (a) –(f) (i.e. protecting national security, collecting taxes etc). Whereas other organisations can only use it for specific purposes – so, the Serious Organised Crime Agency can only use surveillance for purposes (a) – (c) (i.e. to protect national security, prevent crime or in the interests of the economic well-being of the UK). Local councils can use this surveillance for purpose (b) (preventing/investigating crime or disorder).
See SI 2010/521 *Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010* which sets out all the purposes each organisation can use the surveillance (in the Schedule).

Covert Human Intelligence Sources (CHIS)

If a CHIS records or films anything while acting as a CHIS that will not constitute surveillance (so won't need authorisations under the intrusive/directed surveillance rules – just CHIS authorisation)

Method of authorisation

Self-authorised: Authorised by 'designated person' in that organisation (s 29) and the ranks or office of who is able to authorise directed surveillance is as prescribed (s 30).

Must always be a person within the responsible investigating authority who will have day-to-day responsibility for dealing with the CHIS and for their security and welfare. Also need another person within the organisation responsible for the general oversight of the use of the source (s 29(5).

Reason for Authorisation

Can get authorisation if it would be proportionate to do so and necessary for (s 29):

a. National security
b. Prevent/detect crime or prevent disorder
c. In the interests of the economic well-being of the UK
d. Interests of public safety
e. Protect public health
f. Collect taxes, duty etc
g. For anything else specified in an order (none specified to date for CHIS).

Who has access?

Schedule 1, Part 1 of RIPA sets out who has access (can be amended by order). Includes a vast range of bodies including the police, SOCA, intelligence services, HMRC, government departments, all local authorities, fire authorities, Charity Commission, Environment Agency, Financial Services Authority, Food Standards Agency, Gambling Commission, Office of Fair Trading, Gangmasters Licensing Authority, Care Quality Commission etc.

NOTE- the purposes that organisations can use this type of surveillance depends on the particular organisation. So, for example, police forces can use this surveillance for all of the purposes listed in (a) –(f) (i.e. protecting national security, collecting taxes etc). Whereas other organisations can only use it for specific purposes – so, the Serious Organised Crime Agency can only use surveillance for purposes (a) – (c) (i.e. to protect national security, prevent crime or in the interests of the economic well-being of the UK). Local councils can use this surveillance for purpose (b) (preventing/investigating crime or disorder).
See SI 2010/521 *Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010* which sets out all the purposes each organisation can use the surveillance (in the Schedule).

Communications Data

Method of authorisation

Self-authorised: Authorised by 'designated person' in that organisation (s 22) and the ranks or office of who is able to authorise directed surveillance is as prescribed (s 25(2)).

Authorisations to be in writing, or at least to make a record of it (s 23) and last for one month (but can be renewed).

Reason for Authorisation

Can get authorisation if it would be proportionate to do so and necessary for (s 22):

a. National security
b. Prevent/detect crime or prevent disorder
c. In the interests of the economic well-being of the UK
d. Interests of public safety
e. Protect public health
f. Collect taxes, duty etc
g. For the purpose, in an emergency, of preventing death or preventing or mitigating death or injury or damage to a person's physical/mental health
h. For anything else specified in an order – so far orders have also specified (see SI 1878/2006):
    - To assist investigations into alleged miscarriages of justice;
    - To assist in identifying a person who has died or is unable to identify him or herself because of a physical or mental condition (other than one resulting from crime), or to obtain info re next-of-kin.

Who has access?

RIPA sets out: police, SOCA, intelligence services and HMRC (see s 25(1) definition of 'relevant public authority' read with s 22(3)).

Orders include: Financial Services Authority, government departments, Gangmasters Licensing Authority, Gambling Commission, Information Commissioner, Serious

Fraud Office, Royal Mail Group, IPCC, NHS Trusts, fire authorities, Food Standards Agency, all local authorities, Charity Commission, Environment Agency, Health and Safety Executive, Office of Fair Trading, Pensions Regulator etc

NOTE- the purposes that organisations can use this type of surveillance depends on the particular organisation. So, for example, police forces can use this surveillance for all of the purposes listed in (a) –(f). (i.e. protecting national security, collecting taxes etc). Whereas other organisations can only use it for specific purposes – so, the Serious Organised Crime Agency can only use surveillance for purposes (a) – (c) (i.e. to protect national security, prevent crime or in the interests of the economic well-being of the UK). Local councils can use this surveillance for purpose (b) (preventing/investigating crime or disorder).
See SI 2010/521 *Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010* which sets out all the purposes each organisation can use the surveillance for (in the Schedule).

Commissioners

Interception of Communications Commissioner (s 57)

- Must be or have been a judge
- Keeps under review the Secretary of State's powers and duties under Part I of RIPA
- Considers communications data acquisition (and use of encryption powers)
- Commissioner can report to the PM if thinks there has been a contravention of RIPA
- Produces an annual report

Intelligence Services Commissioner (s 59)

- Must be or have been a judge
- Keeps under review the exercise of the Secretary of State's powers under RIPA re the intelligence services and s 5 of the Intelligence Services Act
- Looks at the exercise by the intelligence services of their duties/powers under the Acts

Chief Surveillance Commissioner (s 62)

- Must be a judge, or have been a judge
- Keeps under review everything not covered by the other two Commissioners – powers under Part II and III of RIPA
- Can appoint Assistant Surveillance Commissioner – to provide CSC assistance (s 63) (must be a judge/ or have been a judge)

Investigatory Powers Tribunal (s 65)

- Can investigate anything done by an organisation against a person acting under RIPA
- Can investigate complaints about any alleged conduct by or on behalf of the Intelligence Services
- Is the only appropriate Tribunal for the purposes of s 7 of the HRA for many proceedings – including everything in respect of interception of communications and accessing communications data, and in respect of the other types of surveillance: must go to IPT if it is in respect of actions by the intelligence services, police, armed forces, SOCA or HMRC

- There is no right of appeal from a decision by the Tribunal.
- Must hold proceedings in private – under no duty to have any oral hearing
- Full reasons for decision are not given – if you lose you are just told that you lost, if you win you get a summary of the reasons given to you.

Codes of Practice (s 72)

- Duty on person's performing any power or duty under RIPA to comply with Codes – but there can be no civil or criminal proceedings if they don't.
- The Code can be taken into account before a court or tribunal or Commissioner.

WHEN AUTHORISATIONS FOR SURVEILLANCE CAN BE MADE[8]

When authorisation is necessary	Type of surveillance
In the interests of national security	All 5 types of surveillance
For the purpose of preventing or detecting *serious*[9] crime	Interception of communications Intrusive surveillance (not under the 1997 Act) Property interferences under the 1997 Act (i.e. bugging a house by the police)
For the purpose of preventing or detecting any crime *or preventing disorder*	Directed surveillance CHIS Communications Data
For *safeguarding* the economic well-being of the UK	Interception of communications
In the *interests* of the economic well-being of the UK	Intrusive Surveillance Directed surveillance CHIS Communications Data
To give effect to an international mutual assistance agreement to prevent or detect serious crime	Interception of communications
In the interests of public safety	Directed surveillance CHIS Communications Data
For the purpose of protecting public health	Directed surveillance CHIS Communications Data
For the purpose of assessing or collecting any tax, duty , levy or other imposition, contribution or charge	Directed surveillance CHIS Communications Data

[8] Note however that SI 480/2010 and 521/2010 limit which bodies have access to this power for which purpose. So, for example, while the police can use the powers for almost all reasons (i.e. for national security, to protect public health etc) other bodies have limited purposes for its use (i.e. local authorities can use it for the prevention/detection of any crime or disorder, but not to protect national security).

[9] Section 81(2) and (3) of RIPA and section 93(4) of the *Police Act 1997* defines serious in this context as involving violence, or the offence results in substantial financial gain or is conducted by a large number of persons in pursuit of a common purpose or it is an offence for which a person could be reasonably expected to be imprisoned for three years or more.

payable to a government department	
In an emergency, to prevent death or prevent or mitigate injury or damage to a person's physical or mental health	Communications Data
To assist investigations into alleged miscarriages of justice[10]	Communications Data
To assist in indentifying a person who has died or is unable to identify him or herself because of a physical or mental condition (other than one resulting from crime), or to obtain information regarding next-of-kin[11]	Communications Data

[10] See SI 521/2010.
[11] Ibid.