FRAUD FACTS

Fraud Advisory Panel

Issue 11 December 2010

INFORMATION FOR ORGANISATIONS

Overview of the Regulation of Investigatory Powers Act 2000 (RIPA)

The Regulation of Investigatory Powers Act 2000 sets out the statutory investigatory powers available to public authorities. Public authorities need to be aware of the powers available to them and how to conduct investigations in accordance with the Act. Private sector organisations should also be aware of the Act and how it may affect them.

What is RIPA?

The Regulation of Investigatory Powers Act 2000 (RIPA) regulates the use of a range of investigatory powers by public authorities in England, Wales and Northern Ireland in accordance with the United Kingdom's human rights statutory framework.

The Regulation of Investigatory Powers (Scotland) Act 2000 (RIPSA) covers Scotland.

Both Acts contain safeguards to prevent the abuse of investigatory powers.

Purpose

RIPA powers can be authorised for purposes including (but not limited to):

- National security
- Preventing or detecting crime or disorder
- Public safety
- Protecting public health
- Economic well-being of the UK
- Assessing or collecting tax, duty, levy or other imposition.

What activities does it cover?

RIPA covers:

- Interception of communications
- Acquisition of communications data
- Use of covert surveillance (intrusive and directed)
- Use of covert human intelligence sources (CHIS)
- Investigation of electronic data protected by encryption.

Not all powers are available to all public authorities. For example, local authorities are not permitted to use intrusive surveillance, which can only be authorised in relation to serious crime.

Who does it apply to?

Public authorities subject to RIPA include (but are not limited to):

- The police
- Department for Work and Pensions
- Department of Health
- Financial Services Authority
- HM Revenue and Customs (HMRC)
- Serious Fraud Office
- Serious Organised Crime Agency (SOCA)
- Local authorities
- UK Border Agency (UKBA).

A full schedule of public authorities is available in the Act and relevant statutory instruments.

The Act also applies to commercial organisations providing RIPA-prescribed activities, such as covert surveillance, on behalf of public authorities.

Other legislation

Public authorities need to consider other relevant legislation, including (but not limited to):

- Data Protection Act 1998
- Freedom of Information Act 2000
- Human Rights Act 1998
- Police Act 1997
- Police and Criminal Evidence Act 1984
- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

Impact on the private sector

Private sector organisations may be affected by the provisions of RIPA in the following ways:

- They are subject to (or fall within the scope of) a RIPA-regulated investigation conducted by a public authority
- They conduct RIPA-prescribed activities with or on behalf of public authorities.

Organisations may also wish to consider applying the best practice principles and safeguards contained in the Act to any convert investigations they conduct.

Communications

Part I of RIPA regulates the interception of communications such as telephone calls, emails or letters and the acquisition and disclosure of communications data such as communication logs, billing or subscriber information.

The use of interception techniques and the acquisition of communications data is limited to a certain number of specified public authorities including (but not limited to) the police, SOCA, HMRC, UKBA and the intelligence services.

Surveillance

Part II of RIPA regulates the use of covert surveillance (intrusive and directed) and covert human intelligence sources.

Under the Act surveillance is 'covert' if it is carried out in such a way as to ensure that

the persons subject to the surveillance are unaware that it is taking place.

Covert human intelligence sources: Refers to the use of undercover officers or other persons as defined under section 26(8) of RIPA to obtain information as part of an investigation.

Directed surveillance: Is carried out for a specific investigation or operation in a manner likely to obtain private information about a person and is performed otherwise than by way of immediate response to events.

Intrusive surveillance: Is carried out in relation to anything taking place on residential premises or in a private vehicle and involves the presence of a person on the premises or in the vehicle or is carried out by using a surveillance device. For example, placing an audio or visual device inside residential premises or a private vehicle, or using long-range audio or visual equipment which provides the same quality as if the device were in the residence or vehicle.

The use of intrusive surveillance is limited to a certain number of specified law enforcement agencies including (but not limited to) the police, SOCA, HMRC and the intelligence services.

Authorisation

In most circumstances public authorities need to obtain appropriate authorisation and/or warrants before using powers under RIPA. Different levels of authorisation are required, depending upon the type of power sought.

For example, directed surveillance and covert human intelligence sources are authorised by the organisation itself, whereas interception warrants are authorised by the Secretary of State.

Failure to obtain authorisation does not necessarily render the action unlawful, but may result in any evidence gathered being challenged under the Human Rights Act 1998 and deemed to be inadmissible in court (section 78 of Police and Criminal Evidence Act 1984).

Electronic data protected by encryption

Part III of RIPA regulates the investigation of electronic data that has been protected by encryption or passwords.

It permits specified public authorities to require individuals to disclose the contents of protected electronic information in an intelligible form. Failure to comply with a notice of disclosure is a criminal offence.

Codes of practice

Codes of practice covering the main provisions of RIPA and RIPSA are available to download from the Home Office and Scottish Government websites. These codes are designed to assist public authorities to determine when it is appropriate to use covert investigation and surveillance.

Oversight

The Office of Surveillance Commissioners (OSC) provides oversight of the use of covert surveillance and covert human intelligence sources by public authorities under RIPA (Parts II and III), RIPSA and the Police Act 1997.

It reviews authorisations and conducts inspections of police forces and other law enforcement authorities.

Complaints

The Investigatory Powers Tribunal (IPT) investigates complaints from the public about the conduct of public authorities when using powers conferred by RIPA.

Further information

Home Office
www.homeoffice.gov.uk/counter-terrorism/

Investigatory Powers Tribunal
www.ipt-uk.com

Legislation.gov.uk
www.legislation.gov.uk

Liberty (Your Rights)
www.yourrights.org.uk

Office of Surveillance Commissioners
www.surveillancecommissioners.gov.uk

Scottish Government
www.scotland.gov.uk

The Fraud Advisory Panel gratefully acknowledges the contribution of Ian Ross (Fraud Consulting) in the preparation of this Fraud Facts.

Fraud Advisory Panel, Chartered Accountants' Hall, PO Box 433, Moorgate Place, London, EC2P 2BJ.
Tel: 020 7920 8721, Fax: 020 7920 8545, Email: info@fraudadvisorypanel.org.
Registered Charity No. 1108863

Distributed by