The Investigatory Powers Act 2016 (IPA) governs the covert surveillance of electronic and postal communications. This guide provides a general overview of the legislation for those who are new to the subject.

INTRO

AN INTRODUCTION TO UK LEGISLATION | NOVEMBER 2017

FRAUD ADVISORY PANEL

Investigatory Powers Act 2016

INTRODUCTION

There are two key pieces of legislation dealing with UK surveillance. These are:

- **Regulation of Investigatory Powers Act 2000** (RIPA or RIPSA in Scotland); and
- **Investigatory Powers Act 2016** (IPA).

WHAT IS THE IPA?

IPA deals with the powers of public bodies to gain access to the public's communications and communications data in ways that are compliant with the European Convention on Human Rights.

It does not wholly repeal RIPA or RIPSA which remain in force for other types of covert surveillance such as directed and intrusive surveillance and the use of covert human intelligence sources.

WHAT ACTIVITIES DOES IT COVER?

IPA covers:

- interception (accessing communications);
- interference (accessing electronic equipment); and
- retention and disclosure of communications data.

The intelligence services have the most powers. Less intrusive powers (such as access to communications data) are available to a much wider range of public bodies.

INTERCEPTION

Interception is the most intrusive form of surveillance and has the most rigorous authorisation procedures. Criminal and civil sanctions exist for unauthorised use.

Interception occurs when someone other than the sender or intended recipient gains access to a communication while it is in transit (or is still in the system after transmission) and becomes aware of its contents. Examples include draft emails waiting to be sent, sent emails waiting to be opened, voicemail messages, and letters/parcels intercepted and opened en route.

The power to intercept communications is limited to the following specified bodies:

- the intelligence services
- Metropolitan Police Service
- National Crime Agency
- Police Service of Northern Ireland
- Police Service of Scotland
- Her Majesty's Revenue and Customs (HMRC)
- Defence Intelligence
- UK Central Authority on behalf of an overseas government for the purposes of an EU mutual assistance instrument or an international mutual assistance agreement.

They can intercept for: the purposes of national security; preventing or detecting serious crime; the economic well-being of the UK if, in so far as it is relevant to national security, the investigation is into the activities of persons outside the UK, the Channel Islands and the Isle of Man; or giving effect to the provisions of a mutual assistance agreement.

There are restrictions on the interception of communications of MPs and members of the devolved legislatures, communications subject to legal privilege, and confidential journalistic material.

Ensuring material is available
Authorised public bodies can serve technical capability notices on telecommunications operators (such as phone companies, internet service providers, social media platforms and cloud hosts) requiring them to install specified technical facilities so that they can comply with any interception warrant subsequently served on them.

Telecommunications and postal operators, regardless of whether they are in the UK, are under a legally enforceable duty to comply with interception or mutual assistance warrants. It is an offence to knowingly fail to comply.

Procedural requirements
Authorised public bodies seeking an interception warrant apply to the relevant Secretary of State who must satisfy themselves that the interception is both necessary and proportionate for one of the purposes mentioned above, and that adequate safeguards are in place to prevent improper disclosure. The signed warrant application must then be reviewed in writing with regard to the necessity and proportionality by a Judicial Commissioner working for the Investigatory Powers Commissioner, applying the same principles that a court would apply on an application for judicial review.

Only after these requirements have been met can the warrant be served on the communications service provider.

If the Judicial Commissioner refuses to grant the warrant there is a right of appeal to the Investigatory Powers Commissioner.

An interception warrant lasts for six months (unless it is cancelled earlier).

Exclusions from legal proceedings
Under criminal law, material obtained by interception cannot be used in evidence, disclosed (except in very limited circumstances), requested, or even asked about. The fact that an interception has taken place cannot also be disclosed. Unauthorised disclosure of the application for, the contents of, actions taken under, material recovered or even the existence of an interception warrant is an offence.

OTHER FORMS OF LAWFUL INTERCEPTION (NO WARRANT REQUIRED)

Interception with the consent of the sender or recipient
Communications may be intercepted without a warrant if both the sender and the intended recipient have given consent; or if either the sender or the intended recipient has consented and directed surveillance has been authorised under Part 2 of RIPA.

Interception by providers of postal or telecommunications services
A telecommunications or postal service provider can intercept its own services in connection with the operation of that service. For example, opening a letter or parcel to determine the address of the sender because there appears to be an incorrect delivery address, or filtering out adult material on an internet search engine, or to maintain the integrity of their services and ensure the security of their customers.

Interception by businesses for monitoring and record-keeping
The Secretary of State can make regulations to authorise interceptions which are a legitimate business practice. For example, recording telephone conversations for training or quality control purposes.

Customs
HMRC has the power to intercept postal items under section 159 of the Customs and Excise Act 1979, or Schedule 7 of the Terrorism Act 2000.

Office of Communications
Ofcom has power to intercept communications in exercising certain functions, including the granting of wireless telegraphy licences and preventing and detecting interference with wireless telegraphy.

Prisons, psychiatric institutions and immigration detention facilities
Statutory provisions exist relating to prisons, psychiatric institutions and immigration detention facilities which provide powers to intercept communications to and from those institutions.

Interception in accordance with overseas requests
A telecommunications or postal operator may intercept the communications of an individual at the request of another country even if that person is outside the UK or believed to be so.

ACCESS TO COMMUNICATIONS DATA

Designated public bodies have considerable powers to access the communications data surrounding messages including:

- Entity data: which relates to people and things such as ISP addresses, phone numbers etc.
- Events data: things that have happened such as the fact that someone has sent or received a text and their location at the time.

A large number of public bodies have these powers including (but not limited to) the Financial Conduct Authority, Serious Fraud Office and local authorities.[1]
A full list is available in Schedule 4 to IPA.

Ensuring data is available
The Secretary of State (with the approval of a Judicial Commissioner) may issue a retention notice requiring a telecommunications operator to retain communications data for a maximum period of 12 months so that it is available to public bodies.

Procedural requirements
A public authority can be authorised to access communications data if a designated senior officer (DSO) of the specified rank or grade within that body – independent of the investigation for which the information is being sought – certifies that the request is necessary and proportionate for one of the purposes listed in IPA s.61(7) including (but not limited to) national security, preventing or detecting crime or preventing disorder, and public safety.

Access to entity data is considered less intrusive than access to events data. This means that entity data authorisations are sometimes granted by a less senior officer.

Public bodies must appoint a trained senior person to act as the single point of contact (SPoC) with communication providers. This person may also be the DSO, though these roles are usually split.

Journalistic sources
Data requests to identify a journalistic source need the prior approval of a Judicial Commissioner.

Collaboration agreements
Relevant public bodies may (and, in the case of local authorities, are required to) enter into collaboration agreements to pool resources during busy periods or where public bodies make infrequent requests.

Under the Police Act 1997 the police are permitted to be party to a collaboration agreement. The National Crime Agency (NCA) can be party to a police collaboration agreement.

Preventing 'tipping off'
It is a criminal offence if a communications service provider without reasonable excuse discloses the existence of a data authorisation to the subject of the authorisation. Reasonable excuse includes disclosure with the permission of the public authority that requested the data.

EQUIPMENT INTERFERENCE

Equipment interference occurs when intelligence or law enforcement agencies 'hack' computers, media devices (CDs, USBs etc.) or smartphones to gain access to the contents (activities that would ordinarily be offences under the Computer Misuse Act 1990). Examples include gaining remote access to computers to covertly download the contents of a mobile phone or storage media during a search.

This power is available to the intelligence services, police forces and certain public bodies as listed in Schedule 6 to IPA.

It is used as a way of gathering intelligence material within the UK that might not be susceptible to interception because, for example, it is sent in encrypted format. It is not the same as the forensic analysis of seized material using the existing search and seizure powers available to law enforcement agencies.

BULK INFORMATION GATHERING

Intelligence agencies (but no one else) can seek warrants to carry out bulk information gathering on unspecified people or premises outside of the UK without the need to go into the specific detail required for UK interception applications.

It is inevitable that some communications between individuals in the UK will also be intercepted. A targeted examination warrant must be sought to examine the content of those communications.

According to MI5, bulk communication data has played a part in every major counter-terrorism operation over the last decade.

BULK PERSONAL DATASETS

Intelligence agencies may seek warrants to retain bulk personal datasets such as the electoral roll, telephone directories or travel-related data. This material is used to establish links between people and groups of intelligence interest.

OVERSIGHT

The Investigatory Powers Commissioner (IPC) provides oversight of the use of all surveillance by bodies under RIPA, RIPSA, IPA and the Police Act 1997.

Judicial Commissioners working for the IPC review and, if appropriate, approve surveillance authorisations and conduct inspections of public bodies that use surveillance powers.

THE INVESTIGATORY POWERS TRIBUNAL

The IPT is a court which investigates and determines complaints about the use of surveillance powers by public bodies (including law enforcement). There is a right of appeal to the Court of Appeal.

FURTHER INFORMATION

Available from the **resources** section of our website:

- Regulation of Investigatory Powers Act 2000 (2nd edition)

Other resources

- **Gov.uk**
- **Investigatory Powers Tribunal**
- **Legislation.gov.uk**
- **National Technical Assistance Centre**
- **Scottish Government**

ACKNOWLEDGEMENTS

Thanks to Gary Adams for his valuable contribution to this guide.

NOTES

[1] Local authorities can only obtain communications data for preventing or detecting crime or preventing disorder.

FRAUD ADVISORY PANEL

Chartered Accountants' Hall
Moorgate Place
London EC2R 6EA UK

T +44 (0)20 7920 8721
E info@fraudadvisorypanel.org
www.fraudadvisorypanel.org

Charity Registered in England and Wales No. 1108863
Company Limited by Guarantee Registered in England and Wales No. 04327390