

# Surveillance Law and RIPA

Ibrahim Hasan  
*Act Now Training*



---

---

---

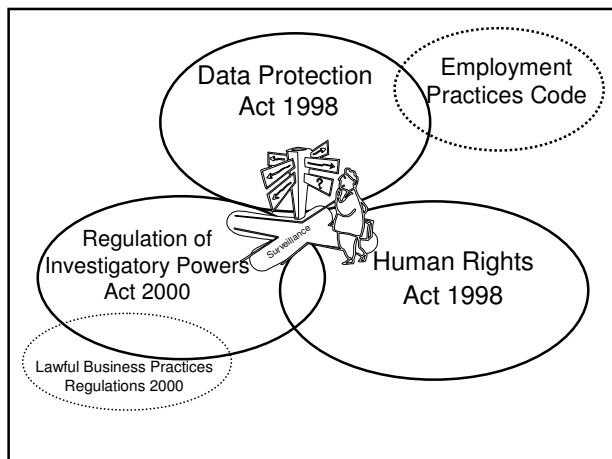
---

---

---

---

---



---

---

---

---

---

---

---

---

## What is RIPA?

1. Interception of Communications
2. Acquisition of Communications Data
3. Surveillance & Covert Human Intelligence Sources (CHIS)
4. Disclosure of Encrypted Data
5. Scrutiny

---

---

---

---

---

---

---

---

## Background

- Interception of Communications Act 1985
- Halford v United Kingdom
- Human Rights Act 1998
- Permissive Legislation (S.80)

---

---

---

---

---

---

---

---

## Section 80

Nothing in any of the provisions of this Act by virtue of which conduct of any description is or may be authorised by any warrant, authorisation or notice, or by virtue of which information may be obtained in any manner, shall be construed-

- (a) as making it unlawful to engage in any conduct of that description which is not otherwise unlawful under this Act and would not be unlawful apart from this Act;
  - (b) as otherwise requiring-
    - (i) the issue, grant or giving of such a warrant, authorisation or notice, or
    - (ii) the taking of any step for or towards obtaining the authority of such a warrant, authorisation or notice,
- before any such conduct of that description is engaged in; or
- (c) as prejudicing any power to obtain information by any means not involving conduct that may be authorised under this Act.

---

---

---

---

---

---

---

---

## Case No: IPT/03/32/H

– 14<sup>th</sup> November 2006

“Although RIPA provides a framework for obtaining internal authorisations of directed surveillance (and other forms of surveillance), there is no general prohibition in RIPA against conducting directed surveillance without RIPA authorisation. RIPA does not *require* prior authorisation to be obtained by a public authority in order to carry out surveillance. Lack of authorisation under RIPA does not necessarily mean that the carrying out of directed surveillance is unlawful.”

---

---

---

---

---

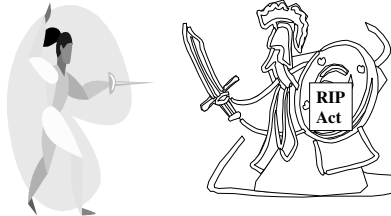
---

---

---

### The RIPA Shield

- Judicial Review
- Article 8
- Article 6
- PACE



---

---

---

---

---

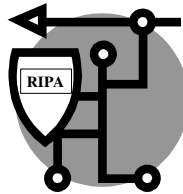
---

---

---

### The RIPA Shield

Section 27 (a) “lawful for all purposes.”  
(b) no civil liability re: incidental conduct



---

---

---

---

---

---

---

---

### Human Rights Act 1998

2nd October 2000

---

---

---

---

---

---

---

---

### The Convention Rights

- Art 1 - duty to secure rights & freedoms
- Art 2 - right to life
- Art 3 - prohibition on torture
- Art 4 - prohibition on slavery
- Art 5 - right to liberty and security
- Art 6 - right to a fair trial
- Art 7 - protection from retroactive criminal offences

---

---

---

---

---

---

---

---

### The Convention Rights

- Art 8 - right to privacy
- Art 9 - freedom of religion
- Art 10 - freedom of expression
- Art 11 - freedom of assembly
- Art 12 - right to marry
- Art 13 - right to an effective remedy
- Art 14 - freedom from discrimination

---

---

---

---

---

---

---

---

### The Act & Local Authorities

#### Section 6

“It is unlawful for a Public Authority to act or fail to act (whether deliberately or not) in a way which is incompatible with Convention Rights...”

---

---

---

---

---

---

---

---

### Article 8 - Privacy

“Everyone has the right to respect for his private and family life his home and his correspondence.

There shall be no interference by a public authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interests of public safety, for the protection of public order, health or morals, or for the rights and freedoms of others.”

---

---

---

---

---

---

---

---

### Caselaw

**Privacy**

- Douglas & Zeta-Jones v hello! Ltd (2000)
- David and Victoria Beckham v MGN ltd (2001)
- Naomi Campbell v Mirror Group Newspapers (2002)

**Disclosure of Information**

- Leander v Sweden (1987)
- MS v Sweden (1999)

**CCTV**

- Peck v United Kingdom (2001)

---

---

---

---

---

---

---

---

### Key Human Rights Concepts

- Necessity
- Proportionality
- Collateral Intrusion

---

---

---

---

---

---

---

---

**Key Human Rights Concepts**

- Necessity
- Proportionality
- Collateral Intrusion

---

---

---

---

---

---

---

---

**Key Human Rights Concepts**

- Necessity
- **Proportionality**
- Collateral Intrusion

---

---

---

---

---

---

---

---

**Covert Surveillance Code (Para 2.5)**

“ This involves balancing the intrusiveness of the activity on the target and others who might be affected by it against the need for the activity in operational terms. The activity will not be proportionate if it is excessive in the circumstances of the case or if the information which is sought could reasonably be obtained by other less intrusive means. All such activity should be carefully managed to meet the objective in question and must not be arbitrary or unfair.”

---

---

---

---

---

---

---

---

### DCA HR Guide (Pg 55)

“ When taking decisions that may affect any of the qualified rights, a public authority must interfere with the right as little as possible only going as far as is necessary to achieve the desired aim.”

- See R v. Secretary of State for the Home Department ex p Daly (2001)

---

---

---

---

---

---

---

---

### Is it Proportionate?

- |   |  |
|---|--|
| <ul style="list-style-type: none"><li>• Is the surveillance excessive in the circumstances?</li><li>• Is it arbitrary or unfair?</li><li>• Can you get information using less intrusive means/ overt methods?</li><li>• What other means have you tried?</li><li>• Factors to set out :<ul style="list-style-type: none"><li>- Amount of data to be gathered</li><li>- Impact on subject of surveillance</li><li>- Timing of surveillance</li><li>- Effect on others (Collateral Intrusion)</li></ul></li></ul> | <ul style="list-style-type: none"><li>• What you are seeking to achieve?</li><li>• Seriousness of the offence</li><li>• Impact of the offence on :<ul style="list-style-type: none"><li>- the victims</li><li>- others/wider community</li><li>- on the public purse</li></ul></li></ul> |
|---|--|

---

---

---

---

---

---

---

---

### Key Human Rights Concepts

- Necessity
- Proportionality
- **Collateral Intrusion**

---

---

---

---

---

---

---

---

### Covert Surveillance Code

2.7 An application for an authorisation should include an assessment of the risk of any collateral intrusion. The authorising officer should take this into account, when considering the proportionality of the surveillance.

2.8 Those carrying out the surveillance should inform the authorising officer if the investigation or operation unexpectedly interferes with the privacy of individuals who are not covered by the authorisation. When the original authorisation may not be sufficient, consideration should be given to whether the authorisation needs to be amended and reauthorised or a new authorisation is required.

2.9 Any person granting or applying for an authorisation or warrant will also need to be aware of particular sensitivities in the local community where the surveillance is taking place and of similar activities being undertaken by other public authorities which could impact on the deployment of surveillance.

---

---

---

---

---

---

---

---

### Collateral Intrusion Considerations

What is the impact on third parties?  
How have you tried to minimise it?

Consider :

- Timing of surveillance
- Amount of surveillance
- Method of surveillance
- Sensitivities of local community
- Operations by other public authorities

---

---

---

---

---

---

---

---

### Key Human Rights Concepts

- Necessity
- Proportionality
- Collateral Intrusion

---

---

---

---

---

---

---

---

### Conclusion

- Be aware - human rights angle/overlap
- Prepare justification/records
- Legal Aid - £50m

---

---

---

---

---

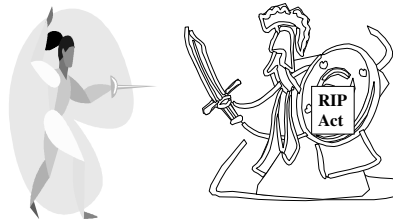
---

---

---

### The RIPA Shield

- Judicial Review
- Investigatory Powers Tribunal
- Article 8
- Article 6
- PACE
- Ombudsman



---

---

---

---

---

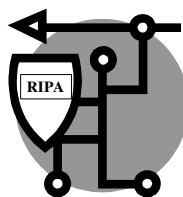
---

---

---

### The RIPA Shield

Section 27 (a) “lawful for all purposes.”  
(b) no civil liability re: incidental conduct



---

---

---

---

---

---

---

---

## Surveillance of People and Places

### RIPA Part 2 :

1. Directed Surveillance
2. Intrusive Surveillance
3. Covert Human Intelligence Sources (CHIS)

---

---

---

---

---

---

---

---

## Directed Surveillance Examples

- Fly tipping
- Benefit fraud
- Anti social behaviour
- Employee surveillance?
- Planning enforcement?

---

---

---

---

---

---

---

---

## Directed Surveillance S. 26 (2)

1. Any covert surveillance that is not intrusive
2. Carried out for the purposes of a specific investigation or operation
3. Likely to result in the obtaining of private information about a person
4. Not an immediate response to events or circumstances where it would not be practical to seek authorisation

---

---

---

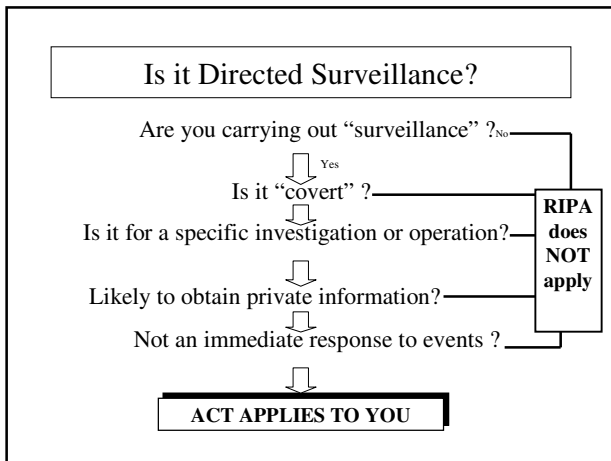
---

---

---

---

---




---

---

---

---

---

---

---

---

**Are You Carrying Out “Surveillance” ?**

“Surveillance” includes:

- Monitoring, observing or listening to persons, their movements, their conversations or their other activities or communication
- Recording anything monitored, observed or listened to in the course of surveillance; and
- Surveillance by or with the assistance of a surveillance device

---

---

---

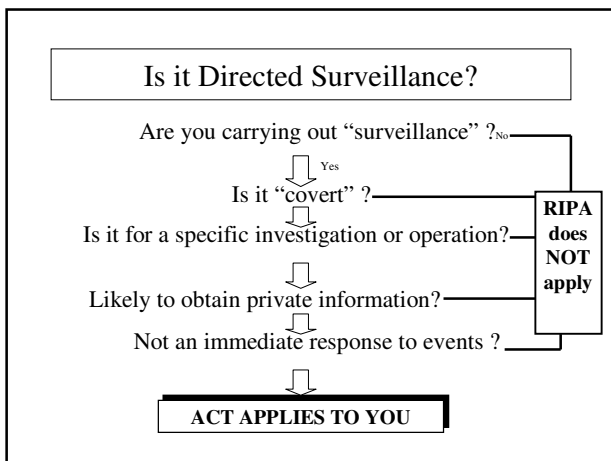
---

---

---

---

---




---

---

---

---

---

---

---

---

### Is the Surveillance “Covert” ?

Section 26 (9)

- Surveillance is covert if, and only if, it is carried out in a manner that is calculated to ensure that persons who are subject to surveillance are unaware that it is or may be taking place
- Dog patrol
- Refuse collection
- Litter enforcement




---

---

---

---

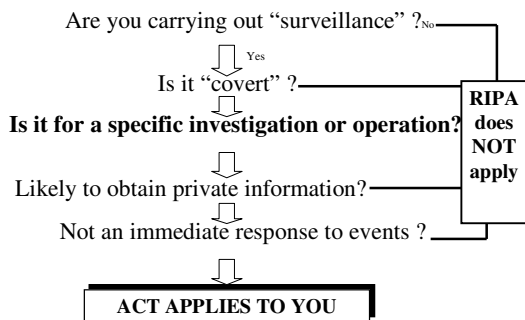
---

---

---

---

### Is it Directed Surveillance?




---

---

---

---

---

---

---

---

### Specific Investigation

Investigatory Powers Tribunal  
 Case No: IPT/03/32/H - 14<sup>th</sup> November 2006  
  
 C v. The Police and Secretary of State for the Home Department

---

---

---

---

---

---

---

---

### Purpose of Directed Surveillance

“Directed surveillance under RIPA is carried out by public authorities which are responsible for the discharge of the specific public functions and are equipped with investigatory powers for the performance of those functions.

Directed surveillance by specified public authorities can only be authorised on specified grounds. Those grounds are linked to the specific public functions of the public authority and vary according to the functions of the particular public authority.”

---

---

---

---

---

---

---

---

### “Core Functions”

“The specific core functions and the regulatory powers which go with them are identifiable as distinct from the ordinary functions of public authorities shared by all authorities, such as the employment of staff and the making of contracts.

There is no real reason why the performance of the ordinary functions of a public authority should fall within the RIPA regime, which is concerned with the regulation of certain investigatory powers, not with the regulation of employees or of suppliers and service providers.”

---

---

---

---

---

---

---

---

### Is it Directed Surveillance?

Are you carrying out “surveillance”? Yes No

Is it “covert”?

Is it for a specific investigation or operation?

Likely to obtain private information?

Not an immediate response to events?

**RIPA  
does  
NOT  
apply**

**ACT APPLIES TO YOU**

---

---

---

---

---

---

---

---

### Private Information S.26(2)

Undertaken in such a manner as is likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purposes of the investigation or operation)

---

---

---

---

---

---

---

---

### Private Information

- 26 (10) - any information relating to a persons private or family life
- Amann v Switzerland (2000) - right to establish and develop relationships with other human beings; incl. professional/business activities
- “Likely” not calculated
- Any person

---

---

---

---

---

---

---

---

### Is it Directed Surveillance?

Are you carrying out “surveillance”? Yes No

Is it “covert”?

Is it for a specific investigation or operation?

Likely to obtain private information?

Not an immediate response to events?

**RIPA  
does  
NOT  
apply**

**ACT APPLIES TO YOU**

---

---

---

---

---

---

---

---

## Immediate Response

“otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation ... to be sought ...”

---

---

---

---

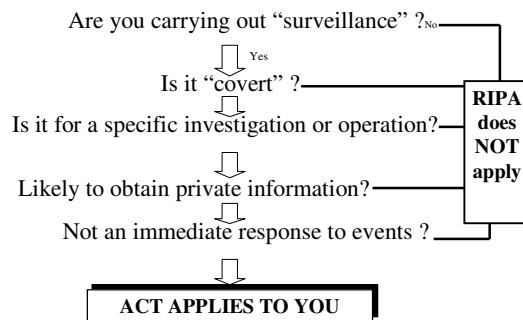
---

---

---

---

## Is it Directed Surveillance?



---

---

---

---

---

---

---

---

## Surveillance & Covert Sources



1. Directed Surveillance
- 2. Intrusive Surveillance**
3. Covert Human Intelligence Sources (CHIS)

---

---

---

---

---

---

---

---

### Intrusive Surveillance s.26(3)

Covert Surveillance that-

(a) is carried out in relation to anything taking place on any residential premises or in any private vehicle; and

(b) involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device

---

---

---

---

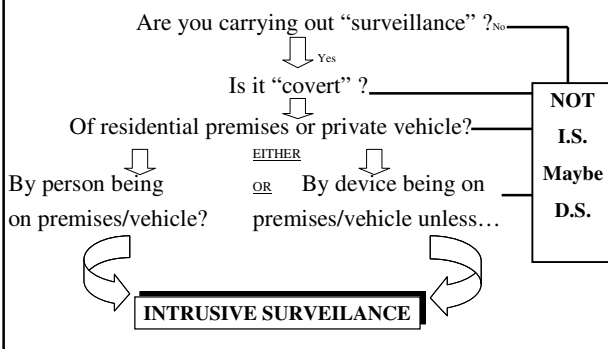
---

---

---

---

### Is It Intrusive Surveillance?




---

---

---

---

---

---

---

---

### Surveillance Device

- Though surveillance device not present on the premises or in the vehicle,
- The device consistently provides information of the same quality and detail as from a device actually present on the premises or in the vehicle.

---

---

---

---

---

---

---

---

### Property Interference

- Part 3 Police Act 1997
- Vehicle Tracking Devices (VTD's)
- Councils have no statutory powers to undertake property interference

---

---

---

---

---

---

---

---

### Intrusive Surveillance

- Check Definition/Flowchart
- Local Authority has no power to carry out intrusive surveillance
- Powers Reserved for Police, HM Customs and Security Services
- Maybe Reviewed

---

---

---

---

---

---

---

---

### CHIS - S.26(8)

A person who

- A. Establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating b or c below
- B. Covertly using such relationship to obtain information or provide access to information
- C. Covertly disclosing information obtained by the use of such a relationship

---

---

---

---

---

---

---

---

### What needs to be authorised?

- Inducing, Asking, Assisting
- Examples:
  - Professional witnesses
  - Test purchases
  - Police informants



---

---

---

---

---

---

---

---

### Volunteers

“The provisions of the 2000 Act are not intended to apply in circumstances where members of the public volunteer information to the police or other authorities, as part of their normal civic duties, or to contact numbers set up to receive information.... “

- Crimestoppers

---

---

---

---

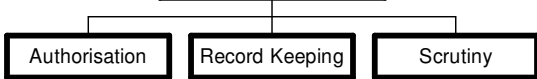
---

---

---

---

### IF RIPA APPLIES



---

---

---

---

---

---

---

---

### Authorisations

- Who can give it?
  - » “Assistant chief officer or service manager or equivalent or any more senior officer...”
  
- What criteria / considerations apply?

---

---

---

---

---

---

---

---

### Confidential Information

- Confidential Personal/Journalistic Material or Legally Privileged information
  
- Inform OSC
  
- Higher Level of Authorisation
  - » “The Head of Paid Service or in his absence a chief officer.”

---

---

---

---

---

---

---

---

### Authorisation Considerations (Directed Surveillance) S.28 (2)

1. Necessary on one of grounds s.28 (3)
2. Proportionate to what is sought to be achieved
3. Collateral Intrusion
4. Confidential Information
5. Review Date

---

---

---

---

---

---

---

---

### Authorisation Grounds

S.28 (3) & S.29(3)

Must be necessary in the interests of :

[1. National security]

**2. Prevention or detection of crime/disorder**

[3. Economic wellbeing of UK]

[4. Public safety]

[5. Protecting public health]

[6. Assessing/collecting tax,duty,levy etc.]

[7. Specified by regulations]      **5<sup>th</sup> Jan 2004**

---

---

---

---

---

---

---

---

### Authorisation Considerations

(CHIS) S.29 (2)

1. Necessary on one of grounds s.29 (3)
2. Proportionate to what is sought to be achieved
3. Special duties S.29 (5)

---

---

---

---

---

---

---

---

### Special Duties S.29 (5)

1. Day to day responsibility for source's security and welfare
2. General oversight of source
3. Record of use
4. Security of source records



---

---

---

---

---

---

---

---

### Authorisations

- Oral grants
- Written grants - forms
- Renewal - statutory review (CHIS)
- Cancellation

---

---

---

---

---

---

---

---

### Central Record

- 3 years – inspection by OSC
- Regulation of Investigatory Powers (Source Records) Regulations 2000, SI No 2725 of 2000
- Confidentiality must be maintained
- Designated person to maintain records
- See codes (paras 2.13/2.14)

---

---

---

---

---

---

---

---

### Central Record Contents

- the type of authorisation;
- the date the authorisation was given;
- name and rank/grade of the authorising officer;
- the unique reference number (URN) of the investigation/operation;
- the title of the investigation or operation, including a brief description and names of subjects, if known;

---

---

---

---

---

---

---

---

### Central Record Contents (2)

- whether the urgency provisions were used, and if so why.
- if the authorisation is renewed, when it was renewed and who authorised the renewal, including the name and rank/grade of the authorising officer;
- whether the investigation or operation is likely to result in obtaining confidential information as defined in this code of practice;
- the date the authorisation was cancelled.

---

---

---

---

---

---

---

---

### Documents to be Retained

- a copy of the application and a copy of the authorisation together with any supplementary documentation and notification of the approval given by the authorising officer;
- a record of the period over which the surveillance has taken place;
- the frequency of reviews prescribed by the authorising officer;
- a record of the result of each review of the authorisation;
- a copy of any renewal of an authorisation, together with the supporting documentation submitted when the renewal was requested;
- the date and time when any instruction was given by the authorising officer.

---

---

---

---

---

---

---

---

### Scrutiny

- Independent Oversight
- 4 Commissioners
  - Interception
  - Intelligence Service
  - Investigatory Powers Commissioner for N I
  - Chief Surveillance Commissioner
- Independent Tribunal



---

---

---

---

---

---

---

---

Common OSC Criticisms

- Use of out of date forms
- Use of cut and paste
- Repetitive narrative and rubber stamping
- Necessity, proportionality and collateral intrusion not fully considered
- Likelihood of obtaining Confidential Information not fully considered
- Central records not compliant with Code e.g URN's etc.
- Inadequate corporate policy/guidance documents
- No CCTV protocol/procedure

---

---

---

---

---

---

---

---

Common OSC Criticisms (2)

- Confusion re: review and renewals
- Lack of understanding of when CHIS
- Monitoring, recording and audit of surveillance equipment
- Handling and storage of surveillance product/evidence
- Confusion about interference with property powers under Police Act 1997
- More robust management and quality assurance
- Lack of regular training/refresher trainer

---

---

---

---

---

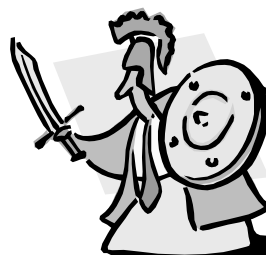
---

---

---

The RIPA Shield

- Judicial Review
- Article 8
- Article 6
- PACE



---

---

---

---

---

---

---

---

### More Information

- Codes of Practice
- [www.homeoffice.gov.uk/ripa/ripact.htm](http://www.homeoffice.gov.uk/ripa/ripact.htm)
- [www.lacors.com.uk](http://www.lacors.com.uk)
- [www.lga.gov.uk](http://www.lga.gov.uk)



---

---

---

---

---

---

---

---

### RIPA Cases

- *Amman v Switzerland* (16/2/00) ECHR 27798/95
- *R v Button and Tannahill* (2005) All ER 75
- *Gilchrist v HM Advocate* (Scotland) Appeal (2004) SCCR595
- *R v E* (2004) EWCA Crim 1243
- *R v Terry and others* (8/8/2001) HH Judge Broderick

---

---

---

---

---

---

---

---

### More RIPA Cases

- *PG and JH v UK* (25/12/01) ECHR 44787/98
- *McGowan v Scottish Water* (2005) IRLR 167
- *Jones v Warwick University* (2003) 3 All ER 760
- *Martin v McGuinness* (2/4/03) (2003) ScotCS 96
- *Grant v R* (4/5/2005) CA Case no: 2003/04573

---

---

---

---


---

---

---

---

### RIPA : Access to Communications Data



---

---

---

---

---

---

---

---

### Background

- Aborted Order in October 2002
- Consultation Paper March 2003
- Draft Order September 2003
- In force 5<sup>th</sup> January 2004

---

---

---

---

---

---

---

---

### The Law

- Part 1 Chapter 2 RIPA
- Section 21-25
- Regulation of Investigatory Powers (Communications Data) Order 2003
- Accessing Communications Data Code of Practice (revised again!)

---

---

---

---

---

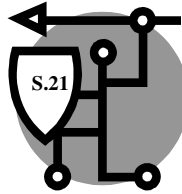
---

---

---

### The RIPA Shield (S. 21)

- (a) “lawful for all purposes.”
- (b) no civil liability re: incidental conduct



---

---

---

---

---

---

---

---

### Who has access

- Police and Security Services
- Fire Authorities
- Ambulance Services
- Local Authorities
- Environment Agency
- Serious Fraud Office
- NHS Bodies
- FSA, DTI, HSE Etc Etc...

---

---

---

---

---

---

---

---

### What kind of data can be accessed?

---

---

---

---

---

---

---

---

### Communications Data (S.21)

- Traffic data
  - Service use data
  - Subscriber data
- Not content of communications

---

---

---

---

---

---

---

---

### Who gets all data?

- Police
- Security Services
- Customs and Excise
- Inland Revenue
- DTI, UKAEAC
- Police Ombudsmen of NI
- FSA }
- Ambulance Services } *Preventing death, injury or damage*
- Fire Authorities } *or crime detection/prevention*

---

---

---

---

---

---

---

---

### Subscriber & Service Use Data

- Government departments
- Local Authorities - *Only for prevention or detection of crime or preventing disorder*
- Fire Authorities – *Prevention of crime or preventing disorder + preventing death or injury*
- Environment Agency – *Only for crime, public safety, public health*
- HSE
- OIC
- OFT

---

---

---

---

---

---

---

---

### Who Decides

- Applicant
- Single Point of Contact (SPOC)
- Designated Person
- Senior Responsible Officer

---

---

---

---

---

---

---

### How to obtain data

- Authorisation
- Notice

---

---

---

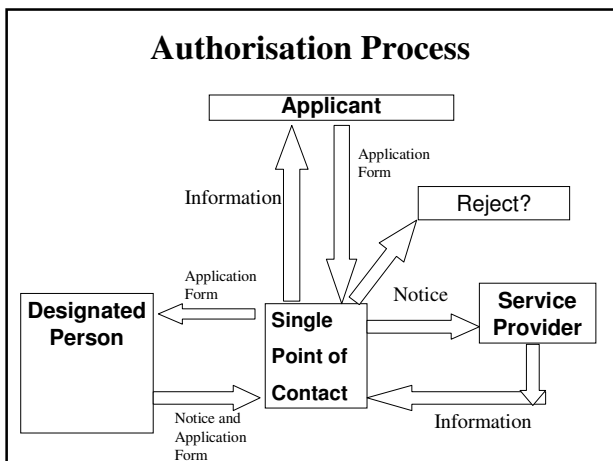
---

---

---

---

### Authorisation Process



---

---

---

---

---

---

---

### Authorisation/Notice Considerations

1. Necessary on one of grounds (S.22)
2. Proportionate
3. Collateral intrusion

---

---

---

---

---

---

---

---

### Necessity Grounds S.22 (2)

Must be necessary in the interests of :

- a) National security
- b) Prevention or detection of crime/disorder**
- c) Economic wellbeing of UK
- d) Public safety
- e) Protecting public health
- f) Assessing/collecting tax,duty,levy etc.
- g) In emergency - preventing death or injury
- h) Specified by regulations

---

---

---

---

---

---

---

---

### Records

- Keep forms till audited
  
- Record dates of commencement and cancellation
  
- Errors must be reported

---

---

---

---

---

---

---

---

## Scrutiny

- Senior Responsible Officer - NEW
- The Interception of Communications Commissioner
- The Tribunal
- Complaints Procedure

---

---

---

---

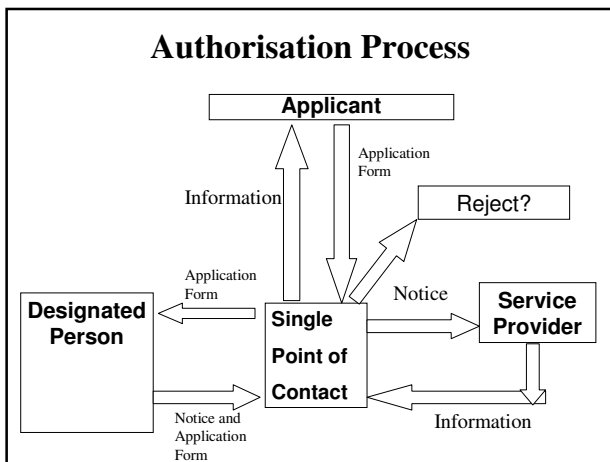
---

---

---

---

## Authorisation Process



---

---

---

---

---

---

---

---

## Interception of Communications



Part 1 Chapter 1  
Section 1-10

---

---

---

---

---

---

---

---

### Misuse By Staff/public

- Downloading
- Bulletin Boards
- Personal use



---

---

---

---

---

---

---

---

### Legal Dangers

Discoverable in court

- Racial/sex discrimination
- Harassment
- Pornography
- Security breaches
- Individual/corporate liability

---

---

---

---

---

---

---

---

### RIP Act 2000

- Public system - criminal offence
- Private system – civil liability



---

---

---

---

---

---

---

---

**RIPA Conditions**

- Consent
- Interception warrant
- Lawful Business Practice Regulations

---

---

---

---

---

---

---

---

**The Telecommunications  
(Lawful Business Practice)  
(Interception of Communications)  
Regulations 2000**

1. Recording evidence of transactions
2. To determine whether or not a communication relates to the business
3. Ensuring compliance with regulatory or self regulatory rules or guidance

---

---

---

---

---

---

---

---

4. Monitoring for purposes of quality control or staff training
5. To prevent or detect crime
6. To investigate or detect unauthorised use of the systems
7. To ensure effective operation of system (i.e. checking for viruses)

NOTE – reasonable efforts to inform users

---

---

---

---

---

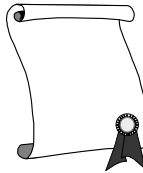
---

---

---

### Policy, Policy, Policy

- Signed or brought to attention of employees
- What can and cannot do with email/internet
- What is surveillance policy?
- No expectation of privacy
- Union consultation



---

---

---

---

---

---

---

---

### The Data Protection Act 1998



---

---

---

---

---

---

---

---

### Does the 1998 Act Apply to You?

Do you process personal data?



ACT APPLIES TO YOU



Notification

8 Principles

Individual Rights

---

---

---

---

---

---

---

---

### Codes of Practice

- CCTV
- Recruitment and Selection
- Employment Records
- Surveillance
- Health Data

---

---

---

---

---

---

---

### Key Provisions

- Initial Assessment Procedure
- Responsible Person
- Purpose of scheme
- Document policy



---

---

---

---

---

---

---

### CCTV Code

- Siting of cameras
- Domestic premises
- Train operators



---

---

---

---

---

---

---

### CCTV Signs

- Clearly visible and legible
- Of an appropriate size
  - car parks A3
  - buildings A4
- Information
  - » identity of controller
  - » purpose of scheme
  - » details of contact



N.B RIPA

---

---

---

---

---

---

---

---

### Key Provisions (2)

- Retention periods
- Subject access
- Third party access – expectation of privacy
- Companies - contract



---

---

---

---

---

---

---

---

### Employment Code Part 3

#### Surveillance

- Point of sales terminals
- CCTV
- E mails
- Auto checking software
- Website logs/Telephone logs
- Vehicle tracking

---

---

---

---

---

---

---

---

### Key Recommendations

- Managing data protection
- The general approach to monitoring: monitoring is intrusive and employees are entitled to keep their private lives private.
- Monitoring should take place for a clear, justified purpose, and employees should be aware that it is taking place.

---

---

---

---

---

---

---

---

### Key Recommendations

- Video and audio monitoring: tell employees
- Covert monitoring: authorisation
- In-vehicle monitoring: develop a policy
- Electronic communications: policy

---

---

---

---

---

---

---

---

### Impact Assessment

- The purposes behind the monitoring;
- Any likely adverse impact on the employee(s) or others
- Alternatives to monitoring, or to the type of monitoring
- The legal obligations that will arise; and
- Whether the monitoring is justified

---

---

---

---

---

---

---

---

### Adverse Impact

- Likely intrusion into employees' private lives
- Extent to which the employee will be aware
- Who will see the information
- Impact on the employment relationship
- The impact on other professionals – e.g. solicitors – who may have confidentiality issues
- How the monitoring will be perceived – e.g. will it be seen as "oppressive" or "demeaning"?

---

---

---

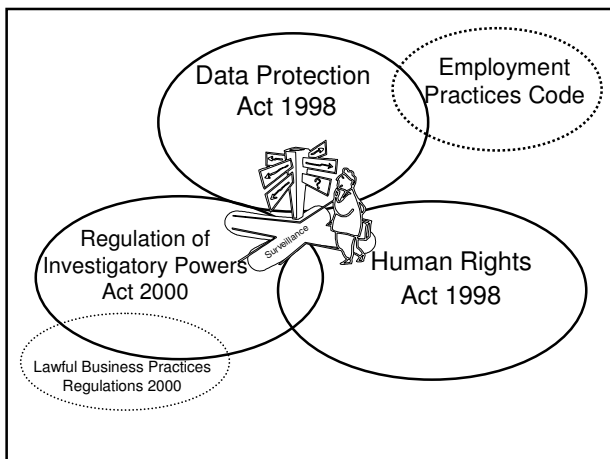
---

---

---

---

---



---

---

---

---

---

---

---

---

### Practical Steps

- Brief management
- Assign responsibility
- Train staff
- Assess documentation
- See the big picture



---

---

---

---

---

---

---

---