RIPA & Local Authorities Virtual Training

- Presenter – David Armstrong, LL.B.
  Barrister at Law.

support@mallard-consultancy.co.uk

Please turn off your microphones until asked to join in

RIPA

- Is it surveillance?
- What is directed surveillance?
- Is it an Article 8 issue?
- Can the evidence be used?
- Overlap with CCTV – DPA

- Since 1 November 2012 two significant changes took effect governing how local authorities use RIPA.

- Approval of Local Authority Authorisations under RIPA by a Justice of the Peace: The amendments in the Protection of Freedoms Act 2012 mean that local authority authorisations and notices under RIPA for can only be given effect once an order approving the authorisation or notice has been granted by a Justice of the Peace (JP).

- Directed surveillance crime threshold: Amendments to the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 ("the 2010 Order") mean that a local authority can now only grant an authorisation under RIPA for the use of directed surveillance where the local authority is investigating particular types of criminal offences. These are criminal offences which attract a maximum custodial sentence of six months or more or criminal offences relating to the underage sale of alcohol or tobacco.

THE TECHNIQUES WHICH LOCAL AUTHORITIES MAY USE:

- Directed surveillance. Local authorities cannot conduct 'intrusive' surveillance (i.e. covert surveillance carried out in residential premises or private vehicles
- CHIS. This can include undercover officers (not simple test purchasing), public informants and people who make test purchases.
- Communications data (CD). This is the 'who', 'when' and 'where' of a communication, but not the 'what' – acquired via a SPOC
- A local authority can only seek the less intrusive types of CD: service use and subscriber information – whilst such falls within the principles of RIPA, the process is distinct from the general RIPA process and is also governed by the Investigatory Powers Act.
- Local authorities cannot be authorised to obtain traffic data under or to intercept the content of any person's communications.

- RANK OF LOCAL AUTHORITY AUTHORISING OFFICERS/DESIGNATED PERSONS

- Local authority authorising officers/designated persons are designated by RIPA consolidating orders SI 2010 Nos.480 and 521, as:

  · Director, Head of Service, Service Manager or equivalent.

- The authorisation of directed surveillance or use of a CHIS likely to obtain confidential information or the deployment of a juvenile or vulnerable person (by virtue of mental or other condition) as a CHIS requires authorisation by the most senior local authority officer – Head of Paid Service or, in his/her absence, the acting Head of Paid Service.

- If there is any doubt regarding sufficiency of rank you should contact your Local Authority Monitoring Officer who will be able to advise you.

- TIME LIMITS:
- The current time limits for an authorisation are:
- 3 months for directed surveillance and
- 12 months for a CHIS (1 month if the CHIS is under 18).

- Authorisations and notices for communications data 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.

- 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 and approved by the JP.

- Applications for renewals should not be made until shortly before the original authorisation period is due to expire but local authorities must take account of factors which may delay the renewal process (e.g. intervening weekends or the availability of the relevant local authority authorising officer and a JP to consider the application).

Crime seriousness threshold

- The crime threshold applies only to the authorisation of directed surveillance by local authorities under RIPA, not to the authorisation of local authority use of CHIS or their acquisition of lower level communications data.

- Local authorities may authorise use of directed surveillance in more serious cases as long as the other tests are met – i.e. that it is necessary and proportionate and where prior approval from a JP has been granted.

- Examples of cases where the offence being investigated attracts **a maximum custodial sentence of six months or more** could include more serious criminal damage, waste dumping and serious or serial benefit fraud.

- Local authorities may also authorise the use of directed surveillance for the purpose of preventing or detecting **specified criminal offences relating to the underage sale of alcohol and tobacco** where the necessity and proportionality test is met and prior approval from a JP has been granted.

Sanctioned by Court

- 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 –

Magistrates' Guidance:

- 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.

IS A RIPA AUTHORISATION REQUIRED?

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.**

- C. vs. The Police
- IPT/03/32 (Investigatory Powers Tribunal)

- This ruling related to whether the Tribunal had jurisdiction under RIPA to determine a claim made by a retired police officer against his former police force. The claim was for unlawful covert surveillance in breach of his right to respect for his private and family life and his home under Article 8 of the European Convention on Human Rights (the Convention) and section 6 of the Human Rights Act 1998 (the 1998 Act). The Tribunal ruled that, as the case related to the use of Private Investigators to undertake directed surveillance in relation to an "employment dispute", no public interest would be served by giving the Tribunal exclusive jurisdiction over such a case. Therefore the Tribunal concluded this was not a case of directed surveillance within RIPA.

- It is common ground that the Tribunal only have jurisdiction in this case if the surveillance alleged by the Applicant is "directed surveillance" within the meaning of sections 26 and 48 (1) and (2).

- Surveillance by public authorities (or, indeed, by anyone else) is not in itself unlawful at common law, nor does it necessarily engage Article 8 of the Convention. For example, general observation of members of the public by the police in the course of carrying out their routine public duties to detect crime and to enforce the law is lawful. It does not interfere with the privacy of the Page 12 individual citizen in a way that requires specific justification

- Did the police actions of which the Applicant complains amount to surveillance? It is common ground that he was under "surveillance." His movements and other activities were monitored, observed and recorded by the private agents on behalf of the police. The fact that private inquiry agents were used by the police to conduct surveillance on their behalf does not affect the responsibility of the police for the purposes of RIPA.

- The second point is: Was the surveillance covert? It has not been contended that the surveillance was other than covert. The Applicant was unaware that it was taking place. There would be little to be gained in carrying out the Page 13 surveillance at all, if it was not covert

- The third point is: Was the surveillance for a specific investigation or a specific operation? This is the key question.

- The surveillance was carried out for the sole purpose of determining **whether the Applicant was as disabled as he had claimed with regard to the effect of his injury on his daily activities.** The information was sought in connection with the response of the police to his pension appeal.

- The point highlighted by Mr Hooper was that surveillance of an employee in the circumstances of this kind of case is unlikely to justify the use of a procedurally restrictive regime and special safeguards, which are tailored to the needs of the public interest and national security cases that clearly fall within the Tribunal's jurisdiction. This is not such a case.

- In these circumstances, the interpretation to be preferred is one which limits "directed surveillance" under RIPA to the discharge of the public authority's particular public or "core functions" specific to it, rather than the carrying out of "ordinary functions" common to all public authorities, such as employment Page 16 (or its nearest equivalent in the case of the police) and entering into contracts to receive or supply other services.

- 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 consequences of not obtaining an authorisation may be that, where there is an interference by a public authority with Article 8 rights and there is no other source of authority, the action is unlawful by virtue of section 6 of the 1998 Act.**

- Directed surveillance, as defined in RIPA, could plainly include surveillance relating to some employment situations.

- If, for example, an employee was suspected by his public authority employer of criminal activities in the course of his work or activities, which would endanger national security or involve threats to public order, and it was necessary and proportionate for the purposes of an investigation to put him under surveillance, an authorisation of directed surveillance for a specific investigation may be obtained by a relevant public authority under RIPA depending on the grounds which are available to that authority.

- The activities of the agents of the police in this case were certainly covert surveillance for the purpose of obtaining private information about the Applicant, **but they were not, in our view, "directed surveillance" in the sense defined in RIPA.** Although "specific investigation" and "specific operation" used in the description of directed surveillance are expressions capable of a wide meaning, they are subject to limitations implicit in their context in the legislation.

- 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.**

- **There are other ways in which the lawfulness of surveillance by a public authority in the context of a private law relationship, such as employment, may be challenged, if it engages Article 8, as amounting to an interference with the right to respect for private and family life, or if it breaches some other specific statutory requirement or private law right**

X v. LOCAL AUTHORITY IPT/03/50/CH

- Following complaints of persistent dog fouling in an upper communal balcony to a block of council flats, a local authority installed a hidden video camera in the balcony area for a 28-day period in order to obtain evidence identifying the offender. No authorisation under the Regulation of Investigatory Powers Act 2000 ('RIPA') was sought

- The Complainant, who at the relevant time lived in one of the flats on the balcony under surveillance, complained to his local authority that the video camera was pointing at his doorway.

- The case did not set a precedent that directed surveillance against dog fouling is never proportionate – simply that in this case **what was represented as general monitoring of a crime 'hotspot' amounted to directed surveillance within the meaning of RIPA as the camera was trained on the suspected offender's front door.**

CCTV – the Code: DPA & POFA

- The unwarranted use of CCTV and other forms of surveillance cameras has led to a strengthening of the regulatory landscape through the passing of the Protection of Freedoms Act (POFA). The POFA has seen the introduction of a new surveillance camera code issued by the Secretary of State since June 2013 and the appointment of a Surveillance Camera Commissioner to promote the code and review its operation and impact.

- The majority of surveillance systems are used to monitor or record the activities of individuals, or both. As such they process individuals' information – their personal data. Most uses of surveillance systems will therefore be covered by the DPA and the provisions of the code, whether the system is used by a multinational company to monitor entry of staff and visitors in and out of its premises, or a local newsagent recording information to help prevent crime.

- This code also covers the use of camera related surveillance equipment including:
  - Automatic Number Plate Recognition (ANPR);
  - body worn video (BWV);
  - unmanned aerial systems (UAS); and
  - other systems that capture information of identifiable individuals or information relating to individuals.

- Using surveillance systems can be privacy intrusive. They are capable of placing large numbers of law-abiding people under surveillance and recording their movements as they go about their day-to-day activities.

- You should therefore carefully consider whether or not to use a surveillance system. The fact that it is possible, affordable or has public support should not be the justification for processing personal data.

- You should consider these matters objectively as part of an assessment of the scheme's impact on people's privacy. The best way to do this is to conduct a privacy impact assessment.

- Recorded material should be stored in a way that maintains the integrity of the information. This is to ensure that the rights of individuals recorded by surveillance systems are protected and that the information can be used effectively for its intended purpose. To do this you need to carefully choose how the information is held and recorded and ensure that access is restricted. You will also need to ensure that the information is secure and where necessary, encrypted. **Encryption can provide an effective means to prevent unauthorised access to images processed in a surveillance system. However, there are circumstances where it is not possible to apply encryption.**

Evidence provided by 3rd Party – Possible breach in recording beyond the home premises

- It is not for the local authority to determine whether the witness has acted entirely lawfully. I would go further in noting that the ICO does not determine that video that may catch views of pavement outside the premises is *necessarily* unlawful. That is a matter for the ICO to determine on the facts and it is quite likely (experience suggests) that the ICO would decline to investigate a matter such as this. That said, it is largely immaterial to the question of admissibility of evidence.

- Let us consider the sentiment of Lord Diplock in the House of Lords in R v Sang where he asserted that it is no function of a criminal court to refuse to admit evidence as a means to sanction a prosecutor in terms of the means by which they obtain evidence. The Court will only act where there is a potential that there may thereby be prejudice to the fairness of trial.

The accepted formulation is as follows –

Kuruma v R [1955]:

- "The test to be applied in considering whether evidence is admissible is whether it is relevant to the matters in issue. If it is, it is admissible and the court is not concerned with how it was obtained."

- This formula was re-stated and approved in R v Khan [1994] and many other cases since.

- Where the evidence is simply submitted by a complainant, there can be no possible further argument of bad faith or oppressive conduct on the part of the prosecutor.

- Note also that the majority of cases where evidence has been obtained directly by the police in contravention of RIPA has nevertheless been admitted in the criminal case, unless there has been a further argument of concurrent abuse of process. This is because Article 8 is subsumed by the Article 6 right to a fair trial.

POLICE NATIONAL BWV GUIDANCE (College of Policing):

- BWV can be very effective for recording the location of objects and evidence at the scene of a crime or during the search of premises. Investigating officers are then able to review, for example, scenes of serious crime, or record the positions of vehicles and debris at the scene of a serious road traffic collision.
- In addition, BWV can be used to provide evidence of the conduct of the search, to confirm where items were found and to record significant statements made by persons present at the scene.
- When used in this way the BWV recording should be treated as an evidential recording and, where possible, the user should provide a running commentary of factual information to accompany the recording to provide context during the review.
- Evidentially and for the purposes of continuity, all officers equipped with BWV and engaged in a search should ensure that their BWV equipment is switched on and recording prior to entering the premises and remains so during the entire searching process.

Residential Premises

- Under normal circumstances, officers should not use BWV in private dwellings. However, if a user is present at an incident in a private dwelling and is there for a genuine policing purpose, they are entitled to make a BWV recording in the same way as they would record any other incident.

- Under Article 8 of the ECHR, individuals have a right to respect for private and family life. Using BWV in a dwelling is always likely to be particularly intrusive, especially during the times of day when occupants are likely to be in bed. Users should, therefore, exercise discretion and record only when it is relevant to the incident and necessary for gathering evidence.

Domestic CCTV – ICO Guidance

- Using CCTV at your home
- If you set up a system so that it captures only images within the boundary of your private domestic property (including your garden), then the data protection laws will not apply to you.
- But if your system captures images of people outside the boundary of your private domestic property – for example, in neighbours' homes or gardens, shared spaces, or on a public footpath or a street – then the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA18) will apply to you, and you will need to ensure your use of CCTV complies with these laws.
- The phrase 'domestic CCTV system' refers to the use of any video surveillance equipment mounted or fixed on your home. It can include cameras fitted to doorbells.

- If capturing images beyond your property boundary, you should have a clear and justifiable reason for doing so. **You will need to**:

- Let people know you are using CCTV by putting up signs saying that recording is taking place, and why.
- Ensure you don't capture more footage than you need.
- Ensure the security of the footage captured.
- Only keep the footage for as long as needed.
- Ensure the CCTV system can't be misused for other reasons.
- Respond to subject access requests (SARs). Individuals have a right to access the personal data you hold about them, including identifiable images. They can ask verbally or in writing. You must respond within one month and give them a copy of the data.
- Deleting footage of people if they ask. This must be done within one month. You can refuse to delete it if you specifically need to keep it for a genuine legal dispute – in which case you need to tell them this, and also tell them they can challenge this in court or complain to the ICO.

SURVEILLANCE AND HUMAN RIGHTS
Code of Practice, August 2018

- **Directed surveillance**

- 3.1 Surveillance is directed surveillance if the following are all true:
  - it is covert, but not intrusive surveillance;
  - it is conducted for the purposes of a specific investigation or operation;
  - it 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);
  - it is conducted 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 under Part II of the 2000 Act to be sought.

- 3.2 Thus, the planned covert surveillance of a specific person, where not intrusive, would constitute directed surveillance if such surveillance is likely to result in the obtaining of private information about that, or any other person (collateral intrusion).

- 2.24 Where covert surveillance activities are unlikely to result in the obtaining of any private information about a person, no interference with Article 8 rights occurs and an authorisation under the 2000 Act is therefore not applicable and this code does not apply. It should be assumed that intrusive surveillance will always result in the obtaining of private information.

- **Private information**

- 3.3 The 2000 Act states that private information includes any information relating to a person's private or family life. As a result, private information is capable of including any aspect of a person's private or personal relationship with others, such as family and professional or business relationships.

- Information which is non-private may include publicly available information such as books, newspapers, journals, TV and radio broadcasts, newswires, web sites, mapping imagery, academic articles, conference proceedings, business reports, and more. Such information may also include commercially available data where a fee may be charged, and any data which is available on request or made available at a meeting to a member of the public. Non-private data will also include the attributes of inanimate objects such as the class to which a cargo ship belongs.

Public Places

- 3.4 Whilst a person may have a reduced expectation of privacy when in a public place, covert surveillance of that person's activities in public may still result in the obtaining of private information. This is likely to be the case where that person has a reasonable expectation of privacy even though acting in public and where a record is being made by a public authority of that person's activities for future consideration or analysis. Surveillance of publicly accessible areas of the internet should be treated in a similar way, recognising that there may be an expectation of privacy over information which is on the internet, particularly where accessing information on social media websites.

- Example –
- *Officers of a local authority wish to drive past a café for the purposes of obtaining a photograph of the exterior. Reconnaissance of this nature is not likely to require a directed surveillance authorisation as no private information about any person is likely to be obtained or recorded. However, if the authority wished to conduct a similar exercise, for example to establish a pattern of occupancy of the premises by any person, the accumulation of information is likely to result in the obtaining of private information about that person.*

Vehicle Tracking

- Section 26(4) of the 2000 Act provides that the use of surveillance devices designed or adapted for the purpose of providing information regarding the location of a vehicle is not considered to be intrusive surveillance. The use of such devices alone does not necessarily constitute directed surveillance as they do not necessarily provide private information about any individual, but sometimes only supply information about the location of that particular device at any one time.

- **The Internet**
- 3.6 Private information may include personal data, such as names, telephone numbers and address details. Where such information is acquired by means of covert surveillance of a person having a reasonable expectation of privacy, a directed surveillance authorisation is appropriate

- 3.10 It is important that public authorities are able to make full and lawful use of this information for their statutory purposes. Much of it can be accessed without the need for RIPA authorisation; use of the internet prior to an investigation should not normally engage privacy considerations. But if the study of an individual's online presence becomes persistent, or where material is to be extracted and recorded and may engage privacy considerations, RIPA authorisations may need to be considered.

- 3.15 Whether a public authority interferes with a person's private life includes a consideration of the nature of the public authority's activity in relation to that information. Simple reconnaissance of such sites (i.e. preliminary examination with a view to establishing whether the site or its contents are of interest) is unlikely to interfere with a person's reasonably held expectation of privacy and therefore is not likely to require a directed surveillance authorisation. But where a public authority is systematically collecting and recording information about a particular person or group, a directed surveillance authorisation should be considered.

Surveillance

- Specific situations where authorisation is not available

3.40 The following specific activities constitute neither directed nor intrusive surveillance:

• the use of a recording device by a covert human intelligence source in respect of whom an appropriate use or conduct authorisation has been granted permitting him or her to record any information obtained in their presence;…

•the covert recording of noise where the recording is of decibels only or constitutes non-verbal noise (such as music, machinery or an alarm), or the recording of verbal content is made at a level which does not exceed that which can be heard from the street outside or adjoining property with the naked ear. In the latter circumstance, the perpetrator would normally be regarded as having forfeited any claim to privacy. In either circumstance, an authorisation is unlikely to be available;

- The judicial approval mechanism is in addition to the internal authorisation process of assessing necessity and proportionality, completing the RIPA authorisation/application form and seeking approval from an authorising officer/designated person.

Application for Judicial Approval –

- The local authority must provide the JP with a copy of the original RIPA authorisation or notice and the supporting documents setting out the case. This forms the basis of the application to the JP and should contain all information that is relied upon.

- For communications data requests the RIPA authorisation or notice may seek to acquire consequential acquisition of specific subscriber information. The necessity and proportionality of acquiring consequential acquisition will be assessed by the JP.

- The original RIPA authorisation or notice 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 relevant tribunal. The court may wish to take a copy.

- In addition, the local authority will provide the JP with a partially completed judicial application/order form.
- 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 as well.
- The order section of the form will be completed by the JP and will be the official record of the JP's decision.
- The local authority will need to obtain judicial approval for all initial RIPA authorisations/ applications and renewals and the local authority will need to retain a copy of the judicial application/ order form after it has been signed by the JP.
- The hearing will be in private and heard by a single JP who will read and consider the RIPA authorisation or notice and the judicial application/order form. He/she may have questions to clarify points or require additional reassurance on particular matters.
- **The forms 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 in the papers provided.**

Entrapment?

- East Riding of Yorkshire v Dearlove (QBD) 2012
- One of the cases referred to by Lord Nicholls was the decision of the Divisional Court in Nottingham City Council v Amin [2001] 1 WLR 1071. Lord Hoffman in Loosely at paragraph 51 described Amin as **a good example of a straightforward application of the distinction between causing the commission of the offence and providing an opportunity for it to be committed.**

- It does not seem to me that there was, in the conduct of the council's officers, anything that could amount to impermissible entrapment. **They booked the service just as an ordinary member of the public would do. The telephone booking was the equivalent, for this kind of service, of the flagging down of a taxi in Amin.**

Loosely

- Re: the nature and extent of police participation in the crime. The greater the inducement held out by the police, and the more forceful or persistent the police overtures, the more readily may a court conclude that the police overstepped the boundary: their conduct might well have brought about commission of a crime by a person who would normally avoid crime of that kind. In assessing the weight to be attached to the police inducement, regard is to be had to the defendant's circumstances, including his vulnerability. This is not because the standards of acceptable behaviour are variable. Rather, this is a recognition that what may be a significant inducement to one person may not be so to another. For the police to behave as would an ordinary customer of a trade, whether lawful or unlawful, being carried on by the defendant will not normally be regarded as objectionable.

Social Media

- The Chief Surveillance Commissioner in his annual report, published on 4th September 2014, drew special attention to the use of the Internet for investigations, particularly involving social networking sites:

- "2.29 The use of the internet may be required to gather information prior to and/or during an operation, which ***may*** amount to directed surveillance. Whenever a public authority intends to use the internet as part of an investigation, they must first ***consider whether*** the proposed activity is likely to interfere with a person's Article 8 rights, including the effect of any collateral intrusion. Any activity ***likely to interfere with an individual's Article 8 rights*** should only be used when necessary and proportionate to meet the objectives of a specific case…

- 5.30. This is now a deeply embedded means of communication between people and one that public authorities can exploit for investigative purposes. I am reasonably satisfied that there is now a heightened awareness of the use of the tactic and the advisable authorisations under RIPA that should be considered. **Although there remains a significant debate as to how anything made publicly available in this medium can be considered private, my Commissioners remain of the view that the repeat viewing of individual "open source" sites for the purpose of intelligence gathering and data collation should be considered within the context of the protection that RIPA affords to such activity.**"

The Application – Authorising Officers

Box 2. Describe the Purpose of the Specific Operation or Investigation

- Here, the requesting officer should state the reason behind the investigation. For example “the purpose of the operation is to, through the use of CCTV cameras, obtain corroborative evidence that the tenants and/or visitors and/or residents at number 2 Acacia Avenue, Any Town have engaged in instances which have or are likely to cause harassment alarm and distress to the neighbourhood for use in possible proceedings for breach of a Criminal behaviour Order without the need for vulnerable members of the community or witnesses to give direct evidence in Court”.

- The authorising officer must be clear from the application what evidence it is hoped will be obtained. If it is obvious that evidence will not be obtainable from the directed surveillance, the application should be referred to the requesting officer for explanation.

Box 3. Describe in Detail the Surveillance Operation to be Authorised and Expected Duration, including any Premises, Vehicles or Equipment (eg Camera, Binoculars, Recorder) that may be used.

- Particulars of the operation will be given here, addressing each aspect raised in the title of box 3.

- References to maps and the type of surveillance equipment to be used and where it is sited are required to assist the authorising officer in determining whether or not to grant the authorisation.

- For example “authorisation is sought to install covert CCTV camera on the roof of the Housing Office opposite block 1 – 7 Acacia Avenue, as marked “A” on the attached map. The map should clearly identify the location i.e. street and town with a north point. Always imagine you do not know the area and do not know the names of the towns- would you be able to find the location from the plan provided?

- The authorising officer should be able to identify the type of surveillance camera to be used/its surveillance capabilities/zoom settings/ its sight lines or whether it can be angled or set so that its impact/intrusion can be reduced. Can it be set to run at certain times or will it be 24/7 hour observation?).

- The hours of operation should be stated with details of how often the camera will be checked for evidence. By way of example – "The expected duration of the operation will be two weeks commencing from when this investigation is authorised. The sight lines for the camera will be outside the pavement at number 1 and number 3 Acacia Avenue. In addition, a mobile CCTV unit placed covertly in a Micra car purchased for its covert surveillance capability will be parked outside number 3 Acacia Avenue marked "B" on the attached map for the same two week duration. It is envisaged to use the cameras 24 hours a day 7 days a week. The camera in the covert Micra car will be directed outside number 3 and 5 Acacia Avenue for the same period."

Box 4. The Identities where known, of those to be the subject of the Directed Surveillance

- Here, details of names and addresses of the intended subject should be supplied or other information about the subjects as appropriate.

Box 5. Information to be obtained as a result of the Directed Surveillance

- This should contain the information to be obtained as a result of the directed surveillance.

- For example “allegations of anti-social conduct have been made against the occupants of number 2 Acacia Avenue, Any Town, Any Place, and their visitors and residents. It is hoped that independent, corroborative evidence of this anti-social conduct can be captured by the CCTV cameras to corroborate the allegations contained in the logs to date, to form the basis of a possible prosecution for breach of a Criminal Behaviour Order without the need for vulnerable witnesses who have been threatened in the past to attend at Court”

Box 6. Grounds for the Directed Surveillance

- A LOCAL AUTHORITY MAY ONLY AUTHORISE FOR THE PURPOSE OF PREVENTING AND OR DETECTING CRIME OR OF PREVENTING DISORDER.

Box 7. Why this directed surveillance is necessary on the grounds you have identified

- Authorising officers (and requesting officers when they complete this form) should have regard to Code of Practice paragraph 2.4. This states that obtaining an authorisation will only ensure that there is a justifiable interference with an individual's Article 8 Rights if it is necessary and proportionate for these activities to take place.

- It first requires authorising officers to believe that the authorisation is necessary in the circumstances of the particular case for the statutory ground outlined at Box 6. **Authorising officers should ask themselves if the evidence to be obtained could be obtained in any other way? Is the directed surveillance operation really necessary to what the requesting officer is seeking to achieve? If there are less intrusive means of obtaining the information, then an authorisation should not be granted.** For example: is it necessary to have the cameras on for two weeks, when one week may provide the information? Could the camera or observations be made during a lesser period of time rather than 24 hours a day?

Box 8. Details of any Potential Collateral Intrusion and why the Intrusion is unavoidable.

- Describe Precautions you will take to Minimise Collateral Intrusion
- Who else, apart from the subject of the surveillance can be affected by the nature of the surveillance? Any application for authorisation should include an assessment of the risk of the collateral intrusion and this should be taken into account by the authorising officer when considering proportionality.
- Officers should carry out an assessment of what information could be received. Officers should address their mind as to what may be a consequence of the surveillance and have a plan to avoid or minimise any such potential intrusion.
- Any evidence or surveillance obtained which is not relevant to the main proceedings should not be used and will be destroyed as quickly as possible. Any evidence to be used in Court or of relevance that shows people not directly relevant to the investigation should be pixilated out to reduce intrusion into their lives.

Box 9. Explain why this Directed Surveillance is proportionate to what it seeks to achieve.

- How intrusive might it be on the subject of surveillance or others? And why is this intrusion outweighed by the need for surveillance in operational terms or can the evidence be obtained by any other means? (Code paragraph 2.5)

- This involves the authorising officer 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. It will not be proportionate if it is excessive in the circumstances of the case or if the information which is thought could reasonably be obtained by other less intrusive means. Activities should be carefully managed to meet the objective in question and must not be arbitrary or unfair.

- The authorising officer should also be provided with information and address their minds to the nature of the complaints or why it is considered proportionate

Box 10 Confidential Information – Indicate the likelihood of acquiring any confidential information

- It is unlikely in the nature of the surveillance that the Council will do that this box will be completed.

Box 11. Applicant's Details.

Box 12. Authorising Officer's Statement (Spell out the 5 W's – who, what, where, when why and how in this and the following box)

- This is the authorising officer's opportunity to detail what they have understood from the application and detail the limits of the permission which is being granted.

- Here, follow exactly three prompts in the box. Please do not miss any out and please be as full as possible so that anyone examining the authorisation and more importantly, the requesting officers and people carrying out the investigation will know exactly what their parameters are and why you have authorised this in the manner that you have.

Box 13. Explain why you believe the Directed Surveillance is necessary (Code paragraph 2.4).

- Explain why you believe the Directed Surveillance to be proportionate to what is sought to be achieved by carrying it out (Code paragraph 2.5)

Box 14 (Confidential Information Authorisation).

- Supply details demonstrating compliance with Code paragraph 3.1 to 3.12) The relevant authorising officer should seek advice from Legal Advisers before authorising surveillance that may secure confidential information – e.g. medical or legal information.

Date of First Review – Box 15

- Complete this box if review dates after the first reviews are known. If not or inappropriate to set additional review dates then confirm not applicable
- Paragraph 4.21 of the Code of Practice provides that regular reviews of authorisations should be undertaken to assess the need for the surveillance to continue. The results should be recorded on the central record of authorisation.
- There is a need to review authorisations frequently where surveillance provides access to confidential information – significant collateral intrusion.
- The authorising officer must determine how often a review should take place. It should be as frequently as considered necessary and practicable. Therefore, set the date of the first review for when it is thought that the requesting officer should have obtained sufficient information to have achieved the aim of their investigation without unnecessary intrusion or imbalanced intrusion into others lives.

CRIMINAL PROCEEDINGS

Following the cases of R v G.S. and Ors [2005] EWCA 887, unrep. 22/4/05, it is more difficult for the defence to demand the applications and authorisation forms. The Court of Appeal made it clear that the Act provides all the relevant lawfulness safeguards and if there is a challenge all the prosecution has to do is produce the relevant authorisations to the Judge only for his inspection.

- What must be remembered is that a breach of Article 8 does not mean that the material must be excluded as a fair trial could take place under Article 6. It all depends on the circumstances, but the case law leans very heavily towards a requirement of bad faith before an Article 8 violation will have an impact on a criminal trial.

- EFFECT ON EVIDENCE IN CRIMINAL TRIALS –

- *Grant v. R (4/5/2005) CA Case No. 2003/04573*

- Appeal allowed against a conviction for conspiracy to murder. The proceedings should have been stayed as an abuse of process. The decision was based on a finding that there had been deliberate covert surveillance of conversations between the accused and his solicitor, by means of a bug in the police station exercise yard. A process that had led to a purported RIPA authorisation of the surveillance demonstrated a disregard for the proper procedures demanded by RIPA.

- *R v. Button and Tannahill [2005] EWCA Crim 516 (4/3/2005) CA Case No: 2004 00204*

  Audio and video recording of defendants while in police custody. Audio recording had been RIPA authorised; video recording was not authorised. Video record admitted in evidence although common ground that it had been unauthorised and so obtained unlawfully (in breach of s.6 Human Rights Act 1998).

- Argued on appeal that the trial Court was itself in breach of s.6 by admitting the evidence.

- Held that the breach of article 8 related to the intrusion upon private life involved in the covert surveillance. So far as a trial Court is concerned: any such breach of article 8 is subsumed by the article 6 (and P.A.C.E.) duty to ensure a fair trial. The trial judge had not acted unlawfully by admitting the evidence.

- *Abbott & Ors v R. [2005] EWCA Crim 2952 (30 November 2005)*

  Appeal against conviction on grounds (inter alia) that evidence of covert recordings of conversation between defendants while in police custody was wrongly admitted. Trial judge had held (after a voir dire) that the recording had been properly authorised under RIPA, despite some technical breaches of the appropriate procedure.

- “it is plain” that breaches of the code and breaches of article 8 do not of themselves render the evidence inadmissible, but are factors which a judge will take into account when exercising his powers under section 76 and 78 of the Police and Criminal Evidence Act 1984. It was "obvious that the admission of this evidence would not adversely affect the fairness of the proceedings." The decision to admit the evidence upheld.