Covert Social Networking Checks and Surveillance Policy

Lancashire County Council

www.lancashire.gov.uk

Contents

1. Introduction

1.1 The increasing availability of 'open source' information, and in particular private information that individuals posts about themselves or others on social media, means that it has never been easier for an officer of a public authority to unwittingly infringe someone's right to a private and family life as set out in the European Convention on Human Rights (ECHR) and the Human Rights Act 1998. Such an infringement by an employee of Lancashire County Council leaves the Council at risk of a claim for breach of those human rights.

1.2 As a public authority, Lancashire County Council has specific obligations in relation to private information and officers cannot assume that just because information is publicly available it may be gathered and used by the Authority.

1.3 Under the terms of the ECHR, the human rights it sets out can only lawfully be infringed in specified circumstances. Within England and Wales, the legal framework under which those rights can be infringed is the Regulation of Investigatory Powers Act 2000 (RIPA).

Further, more specific guidance is available from the Home Office in the form of the Covert Surveillance and Property Interference, and Covert Human Intelligence Sources Codes of Practice of 2018.

RIPA may only be used by local authorities for the prevention or detection of crime. In practical terms this means that RIPA is normally only used by a team or department within the County Council which has a duty to investigate or enforce criminal legislation BUT it is recommended that a similar "shadow" approach be adopted in other investigations where such information may be gathered and utilised. This enables the authority to demonstrate that proper consideration is given to the necessity and proportionality of activity carried out by officers which may infringe the human rights of individuals.

1.4 It is vital that all officers understand the implications of using material recovered from sources such as the internet and social media, and ensure they abide by legislative requirements and take legal advice at an early stage where necessary. Where officers are undertaking covert activity not for the prevention or detection of crime authorisation may still be appropriate in accordance with the LCC Shadow RIPA Surveillance Policy.

2. Private Information

2.1 Section 26(10) of RIPA defines 'private information' in relation to a person as including "any information relating to his private or family life". Case law has defined this to include anything from obviously private information such as that concerning personal relationships to financial information, information about a person's children or even information about a person's business relationships.

Para 3.13 of the Covert Surveillance and Property Interference Code of Practice provides that 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.

2.2 It should be recognised that even if individuals post information about themselves on social media without any privacy settings, they do not forfeit the right to have that material treated as private information by a public authority. The Covert Surveillance and Property Interference Code of Practice is clear that covert surveillance of information in the public domain may still lead to a public authority obtaining private information. This is particularly so

where a public authority records the information either on one occasion or over a period of time. The key question is whether the individual has a reasonable expectation of privacy in the way the material is gathered, retained or used.

3. Covert Activity

3.1 Covert activity is anything that is done in a manner calculated to ensure that the individual subject to the activity is unaware that it is or might be taking place. It follows that most on-line activity will be covert by its very nature. However, where it is shown that the target of any investigation was made aware of the activity then it is possible that subsequent investigative activity may not be considered to be covert. For example, when warnings are issued about the fact that an investigation is likely to take place. Discussions should be held in those cases as to the necessity for authorisation.

4. Directed Surveillance and Covert Human Intelligence Sources (CHIS)

4.1 Directed surveillance is surveillance activity which is not intrusive, and is carried out for a specific investigation or operation, and which is likely to result in the obtaining of private information about any individual. It follows, as set out in the Covert Surveillance and Property Interference Code that it is important that public authorities are able to make full and lawful use of this information for 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.

However the code also states that gathering information about an individual from an on-line source for a specific purpose, even if done on a one-off basis, may amount to directed surveillance, dependent on the nature of the activity, and the level of detail recorded.

4.2 A CHIS is deployed if a person, being an employee of the County Council or a third party establishes or maintains a personal or other relationship with another person for the covert purpose of:

(a) Using such a relationship to obtain information or to provide access to information to another person, or

(b) Disclosing information obtained by the use of such a relationship or as a consequence of such a relationship.

4.3 A public authority is at risk of breaching an individual's human rights in situations where officers conduct planned covert surveillance (which is not intrusive) on an individual where it is likely that private information will be gathered about them in the process, or use a relationship between an individual and a covert human intelligence source (CHIS) to obtain information about that individual. There is also a risk that private information about a third party may be gathered because of the surveillance or the use of CHIS. This is called collateral intrusion, and can be a particular risk with social media since posts from other individuals may be accessible to officers.

4.4 Intrusive surveillance is covert surveillance that is carried out in relation to anything taking place on residential premises or in any private vehicle, and that involves the presence of an individual on the premises or in the vehicle or is carried out by a means of a surveillance device. **Local Authorities are not permitted to conduct intrusive surveillance.**

5. Permitted Activities

5.1 Open source information available on public databases which individuals know may be searched, may be accessed, stored and use for appropriate purposes in the course of an officer's duties. For example, the electoral register may be searched to confirm a resident's address or the Companies' House database may be searched to confirm the registered address and directors' details of a business.

5.2 The Code specifies that the 'general observation duties' of case officers do not amount to directed surveillance. This is because it is not directed at an individual or particular investigation.

In an on-line scenario such 'general observation duties' would involve, for example, general searches on Facebook in order to determine whether a particular product, such as counterfeit goods or fireworks, was being sold via that medium. At some point in an investigation, the officer will reach a point where authorisation for directed surveillance is required. This will need to be judged on a case-by-case basis, dependent on the facts. An initial check of accounts on Facebook where privacy settings are open is unlikely to require authorisation. paragraph 4.14 of the CHIS Code provides that:

"*Where a website or social media account requires a minimal level of interaction, such as sending or receiving a friend request before access is permitted, this may not in itself amount to establishing a relationship. Equally, the use of electronic gestures such as "like" or "follow" to react to information posted by others online would not in itself constitute forming a relationship. However, it should be borne in mind that entering a website or responding on these terms may lead to further interaction with other users and a CHIS authorisation should be obtained if it is intended for an officer of a public authority or a CHIS to engage in such interaction to obtain, provide access to or disclose information."*

It can be seen therefore that minimal interactions would be likely not to require authorisation. At some point though the activity may reach over into territory where authorisation is advisable.

5.3 Test Purchasing

In some cases, officers may need to adopt a covert identity in the course of their duties. For example, a trading standards officer may use a pseudonym in order to complete an on-line test purchase. Use of disguised purchaser details for such a transaction would not require authorisation. However, if the test purchase undertaken requires greater detailed communication with the seller to obtain more information, authorisation may become necessary.

6. Activities Requiring Authorisation

6.1 The Code requires that a public authority which uses the internet as part of an investigation must consider whether the proposed activity is likely to interfere with an individual's article 8 rights. Once an officer covertly gathers, records and retains private information about an individual to a significant extent and going beyond initial reconnaissance, this is likely to amount to directed surveillance and a RIPA authorisation must be obtained.

6.2 If the purpose of the activity is not the prevention or detection of crime, it may still be appropriate for the Authority to undertake directed surveillance of this nature. This should only be done with an appropriate authorisation from a designated authorising officer from the Trading Standards Service, (Head of Service or Trading Standards Manager) that considers the necessity and proportionality of, and risks involved in, the activity.

6.3 Social media allows the sending of personal messages between individuals and it may be a prerequisite of sending such messages that a friend request is made first. In such circumstances an officer may be establishing a relationship with the individual concerned and if this is to be used to obtain information a CHIS authorisation may be required. It should be noted that the use of a relationship to obtain any information, not just private information, amounts to the deployment of a CHIS.

6.4 Again, if the purpose of the activity is not the prevention or detection of crime it may still be appropriate to enter into a relationship with an individual. This should only be done with appropriate authorisation from a designated authorising officer from the Trading Standards Service (Head of Service or Trading Standards Manager) that considers the necessity and proportionality of and risks involved in the activity.

6.5 Where direct communication is entered into with an online operator, for example negotiations about the purchase of goods, obtaining detailed information about the supplier, arranging to meet for example, in those circumstances it would be advisable to seek authorisation for a CHIS. Any directed surveillance carried out in the presence of the CHIS would not then require additional authorisation.

6.6 Officers should not undertake any on-line investigation or other covert activity in their own name as this could compromise their own personal and data security.

7. Unauthorised Activity

7.1 Any activity which has been undertaken which was not properly authorised must be reported to the Investigatory Powers Commissioner. Any officer who believes they may have conducted unauthorised activity that may have infringed an individual's article 8 rights must report it immediately to their line manager who must then seek advice from Trading Standards.

8. Decision Log

8.1 In all cases where the case officer decides to conduct social networking or internet checks this decision should be recorded and should form part of notes on the case file of any investigation. The information should be subject to the normal considerations of data protection and retention in accordance with corporate policy.

9. Service Specific Examples

9.1 Trading Standards Investigations

Typical scenarios
Enquiries into the sale of counterfeit, misdescribed or unsafe goods over the internet or on social networking sites.

Comment and Advice
In such cases, it is necessary for Trading Standards Officers to act covertly to a certain extent – otherwise the activity can be driven underground and offending goods remain on the market.

Trading Standards need to be able to operate with covert purchaser details, and the Codes of practice themselves recognise that this does not, of itself, require authorisation.

In addition, preparatory checks on social media/Facebook that equate to initial observations would not normally require authorisation.

Authorisation is required where the officer plans to use a covert account to befriend and communicate with the target individual, or carries out checks on sites and accounts on a continuing and systematic basis.

9.2 Employee Misconduct Investigations

Typical scenarios

- An employee is suspected of operating a private business in LCC's time. Allegations made by a third party include evidence by way of invoices demonstrating work has been undertaken privately. It is proving difficult to show that the employee is operating a private business during working hours. The employee has not submitted a declaration of business interest and the large gaps between the invoice numbers suggest that this is the tip of the iceberg and a lot of private work has been undertaken.

- An employee is suspected of being employed by a private company whilst being in full time employment with LCC. Furthermore, the employee is in liaison with the private company as part of LCC duties so the two are intrinsically linked and at the very least, there is a conflict of interest.

Actual Case: An employee was conspiring with a sub-contractor and between them had produced fictitious invoices in relation to non-existent work. The fraud ran into hundreds of thousands of pounds. The case eventually went to trial at Crown Court and the employee was convicted and sentenced to a period of imprisonment. Whilst there was sufficient factual evidence to gain a conviction, it would have been useful to access social media during the investigation to ascertain whether there were any links between the employee and individuals from the sub-contracting company and whether there was evidence of a lavish lifestyle that the employee and his wife were leading. Furthermore, there was always doubt as to whether his wife knew of the fraud and again it would have been useful to look at Facebook accounts etc. to ascertain whether there was any evidence of a lavish lifestyle.

Comment and Advice:
Open source searching on names and addresses could reveal whether an employee has any links to commercial activity, or whether there are any open discussions accessible online. These initial searches and checks could be carried out without authorisation, but bear in mind that initial facebook checks require the officer to be logged in and it would be advisable therefore to have covert accounts for officers to do this on an official basis rather than use their own login.

If the initial checks indicate that there is a significant level of information which is of interest, consideration should be given to systematic collation of material and this should be done under a shadow directed surveillance authorisation UNLESS after discussion with the appropriate line manager it is thought that there is a realistic prospect of criminal proceedings being taken, in which case a RIPA authorisation approved by magistrates should be obtained.

9.3 Children's Social Care

Typical scenarios

Scenarios in Children's Social Care (CSC) that might merit surveillance using social media are likely to fall under the following areas:

- Reasonable grounds to believe that information given by a family as part of the assessment is misleading or untrue e.g. the claimed separation of a couple where domestic abuse is known to be a significant risk factor.
- Possible relationship between child and a known or suspected abusive adult.
- Presence of known risky behaviour, drug taking, drinking etc.
- Persons Posing a Risk to a child said to be present in family relationships.

For example, when CSC have concerns about the welfare of the children in a family, the list of friends on a parent's Facebook profile might reveal individuals who are known to be involved in domestic abuse, sexual offences, substance misuse, etc.

Also, timeline postings or photographs on the parent's Facebook profile could indicate activities that might place the children at risk.

Regarding neglect, an example would be where there are concerns that children are being left unsupervised. Facebook timeline postings and photographs could provide evidence of what parents were doing at particular times and dates.

Comment and Advice:
Open source searching on names and addresses may reveal useful information about target individuals. A Facebook search where privacy settings are open may also reveal useful information. These initial searches and checks could be carried out without authorisation, but bearing in mind that initial Facebook checks require the officer to be logged in it would be advisable to have covert accounts for officers to do this on an official basis rather than use their own login.

If the initial checks indicate that there is a significant level of information that is of interest, it may be that the intention is to raise this at an early stage with the relevant parties. If the intention is to continue to monitor the situation and collate material, this should be done under a shadow directed surveillance authorisation UNLESS after discussion with the appropriate line manager it is thought that there is a realistic prospect of criminal proceedings being taken, in which case a RIPA authorisation approved by magistrates should be obtained.

Where privacy settings on Facebook mean that information is not visible except to "friends", in serious cases it may be appropriate (with authorisation) to use shadow CHIS provisions to seek approval to make a friend request using a covert Facebook account.

Version Control

Named Owner:	Laura Sales: Director Corporate Services
Version Number:	4.00
Date Of Creation:	November 2016
Last Review:	August 2021
Next Scheduled Review:	July 2022
Overview of Amendments to this Version:	Grammatical and formatting amendments only.