

Social Media in Investigations policy

wolverhampton.gov.uk

Social Media in Investigations Policy

Introduction

Social media has become a significant means of communication. Many kinds of information are shared in this way ranging from sensitive personal details, photos, videos and comments to demonstrably open “published” items like jokes and announcements. Social media systems have security settings that allow individuals some control over who can see information they have posted online. Most accounts, however, are left “public” or with only limited restrictions leaving them open to view and to surveillance.

The Investigatory Powers Commissioner (IPC) oversees the use of covert surveillance by designated public authorities based in the UK so that the conduct of covert activities by public authorities is human rights compliant.

Covert Surveillance and Property Interference Revised Code of Practice (August 2018) includes specific advice relating to private information and social media surveillance. (See Appendix 1) and refer to the full code of practice.

The Council is committed to ensuring that all access by its staff to social media for the purpose of investigation is appropriate, proportionate and complies with the legal framework outlined below.

Legislation

Regulation of Investigatory Powers Act 2000, Part II (RIPA): covers directed surveillance, covert human intelligence sources and the use of communications data.

Protection of Freedoms Act 2012 (PoFA): Introduced approval by magistrates and restricts directed surveillance to investigations into offences that carry a minimum six-month sentence known as the crime threshold (with the exception of underage alcohol and tobacco sales).

Policy

All investigating officers when considering access to social media will check:

1. Are offences criminal and do they attract a minimum sentence of 6 months?
2. After initial viewing and assessment of the social media is the investigation likely to be advanced by repeat viewing of the site?

3. If the answer to 1 and 2 above is Yes, then the policy and procedures of CWC Regulation of Investigatory Powers Act Policy should be followed and an application made to the authorising officer. If the investigator has any doubts they should apply anyway.
4. If the answer to 1 above is No, then RIPA cannot be used as local authorities may only use directed surveillance for the prevention and detection of crime. Repeatedly viewing an individual's social media site could infringe their Human Rights and must be avoided.
5. If the answer to 2 above is No there is no need to re-access the social media site and investigation can continue without use of the site.
6. If during the conduct of an investigation the nature of the offence changes to surpass the crime threshold or fall below it, this policy should be consulted and followed afresh.
7. If authorisation is granted and approved, ICTS must be approached to enable access for an appropriate period and terminated on its expiry. Officers in Trading Standards can assist with technical advice
8. Officers of the Council must not create false personae accounts in order to disguise their online enquires, unless authorised to do so under RIPA.
9. This policy applies to officer's personal social media accounts when used for an investigation. They must not be used to circumvent this policy.
10. All officers should be aware that social media companies record access to their sites and retain the data. Exposure of inappropriate access may lead to disciplinary action as well as reputational damage to the Council.

Appendix 1

Covert Surveillance and Property Interference Revised
Code of Practice (August 2018) states:

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.

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.

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 appropriate¹³.

Online covert activity

3.10 The growth of the internet, and the extent of the information that is now available online, presents new opportunities for public authorities to view or gather information which may assist them in preventing or detecting crime or carrying out other statutory functions, as well as in understanding and engaging with the public they serve. 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 obtained from any check is to be extracted and recorded and may engage privacy considerations, RIPA authorisations may need to be considered. The following guidance is intended to assist public authorities in identifying when such authorisations may be appropriate.

3.11 The internet may be used for intelligence gathering and/or as a surveillance tool. Where online monitoring or investigation is conducted covertly for the purpose of a specific investigation or operation and is likely to result in the obtaining of private information about a person or group, an authorisation for directed surveillance should be considered, as set out elsewhere in this code. Where a person acting on behalf of a public authority is intending to engage with others online without disclosing his or her identity, a CHIS authorisation may be needed (paragraphs 4.10 to 4.16 of the Covert Human Intelligence Sources code of practice provide detail on where a CHIS authorisation may be available for online activity).

3.12 In deciding whether online surveillance should be regarded as covert, consideration should be given to the likelihood of the subject(s) knowing that the surveillance is or may be taking place. Use of the internet itself may be considered as adopting a surveillance technique calculated to ensure that the subject is unaware of it, even if no further steps are taken to conceal the activity. Conversely, where a public authority has taken reasonable steps to inform the public or particular individuals that the surveillance is or may be taking place, the activity may be regarded as overt and a directed surveillance authorisation will not normally be available.

3.13 As set out in paragraph 3.14 below, depending on the nature of the online platform, there may be a reduced expectation of privacy where information relating to a person or group of people is made openly available within the public domain, however in some circumstances privacy implications still apply. This is because the intention when making such information available was not for it to be used for a covert purpose such as investigative activity. This is regardless of whether a user of a website or social media platform has sought to protect such information by restricting its access by activating privacy settings.

3.14 Where information about an individual is placed on a publicly accessible database, for example the telephone directory or Companies House, which is commonly used and known to be accessible to all, they are unlikely to have any reasonable expectation of privacy over the monitoring by public authorities of that information. Individuals who post information on social media networks and other websites whose purpose is to communicate messages to a wide audience are also less likely to hold a reasonable expectation of privacy in relation to that information.

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. These considerations apply regardless of when the information was shared online. See also paragraph 3.6.

Example 1: *A police officer undertakes a simple internet search on a name, address or telephone number to find out whether a subject of interest has an online presence. This is unlikely to need an authorisation. However, if having found an individual's social media profile or identity, it is decided to monitor it or extract information from it for retention in a record because it is relevant to an investigation or operation, authorisation should then be considered.*

Example 2: *A customs officer makes an initial examination of an individual's online profile to establish whether they are of relevance to an investigation. This is unlikely to need an authorisation. However, if during that visit it is intended to extract and record information to establish a profile including information such as identity, pattern of life, habits, intentions or associations, it may be advisable to have in place an authorisation*

even for that single visit. (As set out in the following paragraph, the purpose of the visit may be relevant as to whether an authorisation should be sought.)

Example 3: A public authority undertakes general monitoring of the internet in circumstances where it is not part of a specific, ongoing investigation or operation to identify themes, trends, possible indicators of criminality or other factors that may influence operational strategies or deployments. This activity does not require RIPA authorisation. However, when this activity leads to the discovery of previously unknown subjects of interest, once it is decided to monitor those individuals as part of an ongoing operation or investigation, authorisation should be considered.

3.16 In order to determine whether a directed surveillance authorisation should be sought for accessing information on a website as part of a covert investigation or operation, it is necessary to look at the intended purpose and scope of the online activity it is proposed to undertake.

Factors that should be considered in establishing whether a directed surveillance authorisation is required include:

- Whether the investigation or research is directed towards an individual or organisation;
- Whether it is likely to result in obtaining private information about a person or group of people (taking account of the guidance at paragraph 3.6 above);
- Whether it is likely to involve visiting internet sites to build up an intelligence picture or profile;
- Whether the information obtained will be recorded and retained;
- Whether the information is likely to provide an observer with a pattern of lifestyle;
- Whether the information is being combined with other sources of information or intelligence, which amounts to information relating to a person's private life;
- Whether the investigation or research is part of an ongoing piece of work involving repeated viewing of the subject(s);
- Whether it is likely to involve identifying and recording information about third parties, such as friends and family members of the subject of interest, or information posted by third parties, that may include private information and therefore constitute collateral intrusion into the privacy of these third parties.

3.17 Internet searches carried out by a third party on behalf of a public authority, or with the use of a search tool, may still require a directed surveillance authorisation.

Example: Researchers within a public authority using automated monitoring tools to search for common terminology used online for illegal purposes will not normally require a directed surveillance authorisation. Similarly, general analysis of data by public

authorities either directly or through a third party for predictive purposes (e.g. identifying crime hotspots or analysing trends) is not usually directed surveillance. In such cases, the focus on individuals or groups is likely to be sufficiently cursory that it would not meet the definition of surveillance. But officers should be aware of the possibility that the broad thematic research may evolve, and that authorisation may be appropriate at the point where it begins to focus on specific individuals or groups. If specific names or other identifiers of an individual or group are applied to the search or analysis, an authorisation should be considered.

This page is intentionally left blank