Wiltshire Council

Guidance on the Regulation of Investigatory Powers Act 2000 (RIPA) and the use of Social Networking Sites/Social Media

This guidance should be read in conjunction with the council's RIPA policies and procedures, its Protocol for Covert Internet Profile Use – Principles, the statutory codes of practice issued by the Secretary of State, and the Office of Surveillance Commissioners' Guidance (*Procedures and Guidance - Oversight arrangements for covert surveillance and property interference conducted by public authorities and to the activities of relevant sources - July 2016*). It applies to any investigatory work undertaken by officers.

It is recognised that the use of the internet and social networking sites can present useful opportunities for Council staff carrying out investigations. These investigations may relate to the various enforcement roles within the council – for example Planning Enforcement, Licensing, Trading Standards or Environmental Health, but will equally apply to some non-enforcement teams, such as Housing.

Social media has become a significant part of many people's lives, with people regularly using and interacting with many different forms of social media. By its very nature, social media accumulates a sizable amount of private information about a person's life, from their daily routines and whereabouts to specific events. Social media can therefore be a very useful tool both when investigating alleged offences with a view to bringing a prosecution in the courts or when considering other local authority actions. The use of information gathered from the various forms of social media available can go some way to proving or disproving such things as whether a statement made by a defendant, or an allegation made by a complainant, is truthful or not.

However, the fact that digital investigation is routine or easy to conduct does not reduce the need for consideration of human rights, data protection and RIPA principles and, in some cases, the requirement for RIPA authorisation, if available, for the issue being investigated. Whilst much can be accessed without the need for RIPA authorisation, use of the internet and social networking sites for investigative purposes has the potential to amount to covert directed surveillance and can even stray into the territory of Covert Human Intelligence sources (CHIS), and can result in the breaching of an individual's privacy rights under the Human Rights Act (Article 8 - Right to respect for private and family life). For a criminal investigation, evidence obtained contrary to RIPA procedures may be inadmissible, as well as leaving scope for a civil action against the Council. RIPA authorization of the use of social media, when necessary and possible, provides safeguards against such claims.

WHAT ARE SOCIAL MEDIA OR SOCIAL NETWORKING SITES (SNS)?

Social media/SNS encompass a wide range of web-based services typically enabling individuals or businesses to construct a public or semi-public profile or creating a platform for sharing views or information. Typical characteristics include:

- The ability to show a list of other users with whom the primary user shares a connection, often termed "friends" or "followers"
- Hosting capabilities for audio, photographs and video content

They can include community-based web sites, online discussion forums and chat rooms.

Current examples include:

- Facebook
- Twitter
- Instagram
- LinkedIn
- Pinterest

- Google+
- Vine
- Tumblr
- Flickr
- YouTube
- Reddit
- Yammer

However, this is not an exhaustive list and similar or new electronic communication systems are being constantly developed and introduced and would be likely to be caught by the umbrella terms, Social Media/SNS.

PRIVACY SETTINGS

It is worth bearing in mind that RIPA defines private information as:

"*any information relating to a person's private or family life and should be taken generally to include any aspect of a person's private or personal relationship with others, including family and professional or business relationships."*

It should be noted that websites used specifically to advertise goods and services, whilst often not social media or SNS, would fall within that definition. Although there is likely to be a reduced expectation of privacy with this type of site, there is still the possibility of obtaining private information which may subsequently be used in enforcement proceedings and officers should be alert to this.

Most social media services allow users to dictate who can view their activity, and to what degree, through the use of privacy settings. Whilst it is the responsibility of an individual to set privacy settings on such sites to protect from unwanted access to their private information, it is unwise for officers to rely on their own perception of a person's reasonable expectations or a person's ability to control their own personal data.

Information publicly available to all is known as an individual's public profile. Publishing content or information using a public setting means that the individual publishing it is allowing everyone to access and use that private information and to associate it with them. However, this approach should not be seen as tacit agreement by that individual to their being **monitored**, whether by the council or by anyone else. 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. The information is still private information regarding that individual and they still have rights in respect of it.

The opposite of a public profile is a private profile. When a private profile is used an individual does not allow everyone to access and use their content; they control who can view their information. In these circumstances, respect should be given to that person's right to privacy under Article 8 and authorization under RIPA, if available, seriously considered.

It should also be noted that even though a user has set their profile to be private it might be shared by a third party who does have access and who has a public profile. Officers should therefore be alert to this possibility and in such instances care should be taken regarding the use of the private information. Where there is any doubt, advice should be sought.

Conducting an investigation under the Social Media Policy.

The diversity of social media means that it is impracticable to prescribe any threshold for requiring authorisation under RIPA, given all the various scenarios that may exist. Authorisation for directed surveillance or for use of a Covert Human Intelligence Source (CHIS) **may** be required and the decision over whether it is necessary to make an application should be taken pragmatically on a case by case basis. If there is any doubt, refer to a line manager, with assistance from Legal Services if necessary.

Using social media for investigatory purposes, will meet the definition of **"directed surveillance"** if:

- it is covert;

- likely to reveal private information;
- and done with some regularity.

Where there is need to apply on-line to join a platform this may require authorisation for use of a CHIS. This will be dependent on the existence of a "relationship." If the application to join a site is a formality and there is no interaction with a suspect or their group, this will at least require a directed surveillance authorisation.

When using the internet and social media as an investigatory tool, there are 3 main considerations for officers:

(1) What expectation of privacy a user may reasonably have when posting on the Internet;
(2) How covert or overt the officer looking at information on the internet is being.
(3) Whether or not a RIPA or CHIS authorisation is possible and should be obtained.

It should be borne in mind that there is a fine line between general observation, and systematic observation and research. The difference between the two approaches will decide whether a RIPA authorisation should be considered.

There are essentially 3 general **scenarios** when using Social Media as a part of an investigation:

1. **Viewing publicly available postings or websites where the person viewing does not have to register a profile, answer a question, or enter any significant correspondence in order to view.**

   This could be the viewing of a trader's website. In this situation there must be a low expectation of privacy and a **RIPA authorisation would not normally** be required to view or record these pages. However, reviewing such open source sites through **repeated visits** over time to the extent that you might be perceived as **monitoring** the website, **may** require authorisation. Private information can remain private information even when posted on such a website.

2. **Viewing postings on social networks where the viewer has had to register a profile but there is not otherwise a restriction on access.**

   This would include Facebook where there is no need to be accepted as a "friend" to view; for example, where a trader has a "shop window" on Facebook advertising a business and products.

   There are differences between this and the previous scenario. The person who posts information or runs such a website may reasonably expect viewers to work within the terms and conditions of the social networking site. Viewing should therefore normally be conducted in an overt manner i.e. via an account profile which uses your correct name, and email address (which should be a Wiltshire.gov.uk address) or a sanctioned profile[1]. If the posting or website contains no private information a viewing would not engage privacy issues and therefore a RIPA authorisation would not be needed. However, it is possible that a mixture of private and business material is displayed, and as set out above, information relating to business relationships can be private information. The conditions regarding **repeat visits** in the previous scenario are also relevant. The use of covert Facebook accounts to access postings would need to be covered by a RIPA authorisation, most likely through a CHIS application.

   Obtaining a RIPA authorisation will also present an officer with a defence should there be an allegation that they have breached the Computer Misuse Act 1990 – it is an offence to deliberately access unauthorised material.

3. **Viewing postings on social networks which require a "friend" or similar status to view.**

   These are **highly** likely to involve viewing private information. Repeated viewings will constitute directed Surveillance and require a RIPA authorisation.

[1] see Protocol for Covert Internet Profile Use – Principles

This may apply whether or not a "covert" or "overt" account is used, though this is probably best obtained via a CHIS authorisation with the use of a covert profile[2].

An "Overt" account which gains "friend" or similar status may **still require a RIPA authorisation.** It may be that such a status may be given by a default on the part of the person posting or website owner. The officer should be especially sure that their access is being granted as a representative of the Service. For example, on Facebook it is stated that only people who know the person who maintains a profile should send a "friend" request to that profile. A person accepting that friend request may believe the person requesting is an acquaintance that they simply do not recall or know by another name. They still have a justifiable expectation of privacy. While requesting access may not comply with a strict interpretation of Facebook terms and conditions, a clearly identifiable **Service Sanctioned profile[3]** is a way to deal with that expectation of privacy, rather than a more neutral officer based profile. A "Covert" account at this level should only be used in the context of a RIPA authorisation.

Covert surveillance of Social Networking Sites (SNS) - Summary

Whilst it is the responsibility of an individual to set privacy settings to protect unsolicited access to private information, and even though data may be deemed published and no longer under the control of the author, it is unwise to regard it as "open source" or publicly available; the author has a reasonable expectation of privacy if access controls are applied. In some cases data may be deemed private communication still in transmission (instant messages for example). **Where privacy settings are available but not applied the data may be considered open source and an authorisation is not usually required. Repeat viewing of "open source" sites may constitute directed surveillance on a case by case basis and this should be borne in mind.**

If it is necessary and proportionate to covertly access an account, the minimum requirement is an authorisation for directed surveillance. An authorisation for the use and conduct of a CHIS is necessary if a relationship is established or maintained (i.e. the activity is more than mere reading of the site's content).

It is not unlawful to set up a false identity but it is not advisable to do so for a covert purpose without authorisation.

Officers should not adopt the identity of a person known, or likely to be known, to the subject of interest or users of the site without authorisation, and without the explicit consent of the person whose identity is being used, and without considering the protection of that person.

Examples

1. An officer is suspected of undertaking additional employment in breach of their contract of employment. The HR department wish to look at the officer's social media accounts to find out if they show anything that may prove whether this is true or not. The officer has their profile set to public and HR only look at the accounts once. Such activity does not constitute directed surveillance for the purposes of RIPA as the officer's profile is set to public and the accounts are only looked at once.

If, however, the accounts continued to be monitored over a period of time then a directed surveillance RIPA authorisation should be considered. However, as the employee is not committing a criminal offence the criminal threshold is not engaged and authorisation for Directed surveillance is not available. The HR department should take advice from legal services in such a case as any action could still put the Council at risk of an allegation of breach of the Officer's human rights unless the Council can establish that the action was necessary and proportionate

2. An officer claiming compensation for injuries allegedly sustained at work is suspected of fraudulently exaggerating the nature of those injuries. The officer's manager wishes to look at the officer's social media accounts to see if posts can prove or disprove the exaggeration of the claim. The manager is intending to monitor the accounts over a period of time. The account settings are public. The proposed surveillance is likely to result in the obtaining of private information and, as the alleged misconduct amounts to the criminal offence of fraud, directed surveillance RIPA authorisation must be considered. If the officer then changes their account settings to

[2] Protocol for Covert Internet Profile Use – Principles
[3] Protocol for Covert Internet Profile Use – Principles

private the manager should not send a friend request to the officer without first discussing the appropriateness of the next steps with their manager and legal.

3. An individual is suspected of not living at the address they have put down on their child's school admission form to try and get into an excellent school. It is suggested that by looking at their social media accounts it might be possible to find out their true address. If it is likely that no criminal offence has been committed then RIPA cannot be used.

LEGISLATIVE OVERVIEW – LINKS

The following are relevant to this area and the subject of RIPA authorisations overall:

- Wiltshire Council RIPA policies
- Secretary of State and the Office of Surveillance Commissioners Guidance

  https://www.ipco.org.uk/docs/OSC%20PROCEDURES%20AND%20GUIDANCE.pdf
- Regulation of Investigatory Powers Act 2000

  http://www.legislation.gov.uk/ukpga/2000/23/contents
- The Home Office Guidance to Local Authorities on the Protection of Freedoms Act 2012 - Changes to Provisions under RIPA

  https://www.gov.uk/government/publications/changes-to-local-authority-use-of-ripa
- Investigatory Powers Act 2016

  http://www.legislation.gov.uk/ukpga/2016/25/contents/enacted
- The CHIS/covert surveillance codes of practice
  https://www.gov.uk/government/publications/covert-surveillance-and-covert-human-intelligence-sources-codes-of-practice

Further reading:

- Do social workers risk a criminal offense by repeatedly viewing service users' social media?
  https://www.communitycare.co.uk/2017/11/02/social-workers-risk-criminal-offense-repeatedly-viewing-service-users-social-media-posts/
- Social workers using social media to find evidence on service users as lack of guidance leaves knowledge gaps https://www.communitycare.co.uk/2018/11/28/social-workers-using-social-media-find-evidence-service-users-lack-guidance-leaves-knowledge-gaps/
- Facebook, Social Networks and the Need for RIPA Authorisations – Dated but useful
  https://actnowtraining.wordpress.com/2015/09/10/facebook-social-networks-and-the-need-for-ripa-authorisations/