HERTFORDSHIRE COUNTY COUNCIL

USE OF SOCIAL MEDIA IN INVESTIGATIONS

POLICY

Updated May 2018

USE OF SOCIAL MEDIA IN INVESTIGATIONS

POLICY

CONTENTS

1 REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)

1.1 This policy should be read in conjunction with the council's RIPA policies and procedures, as well as the statutory codes of practice issued by the Secretary of State and the Office of Surveillance Commissioners Guidance.

1.2 It applies to any investigatory work undertaken by officers.

1.3 RIPA authorisation of the use of social media provides safeguards if a claim is made under Article 8 of the European Convention on Human Rights (Right to respect for private and family life)

1.4 For a criminal investigation, evidence obtained contrary to procedure may be inadmissible, as well leaving scope for a civil action against the County Council.

1.5 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 information about a person's life, from daily routines to specific events. Their accessibility on mobile devices can also mean that a person's precise location at a given time may also be recorded whenever they interact with a form of social media on their devices.

1.6 Social media can therefore be a very useful tool when investigating alleged offences with a view to bringing a prosecution in the courts or taking other action. The use of information gathered from the various different 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.

1.7 Not all information published on social media is true and care must be taken as to the validity of information recorded. The information obtained must only relate to the investigation being carried out and not for a general "fishing" expedition

2 'SOCIAL MEDIA' IN THIS POLICY

2.1 Social media encompasses a wide and dynamic range of web-based services typically facilitating 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

It includes community based web sites, online discussion forums and chat rooms.

2.2 Current examples include:

- Facebook
- Twitter
- Instagram
- LinkedIn

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

2.3 This is not an exhaustive list and similar or new electronic communication systems are likely to be caught.

3 PRIVACY SETTINGS

3.1 The majority of social media services will allow its users to dictate who can view their activity, and to what degree, through the use of privacy settings.

3.2 The information publicly available is known as an individual's public profile.

3.3 Publishing content or information using a public, rather than a private setting, means that the individual publishing it is allowing everyone to access and use that information and to associate it with them. It should not be seen however as an authority to being monitored by the council. The information is still the property of that individual.

3.4 The opposite of a public profile is a private profile, where a user does not allow everyone to access and use their content, and respect should be shown to that person's right to privacy under Article 8.

3.5 Even though a user has set their profile to be private it might be shared by a third party who has a public profile. Care should be taken in such cases and if there is any doubt about the use of such information discuss it with your manager.

4 THE PRINCIPLES

4.1 The diversity of social media means that it is impracticable to prescribe the threshold for requiring authorisation under RIPA in all of the various scenarios that may exist. Ultimately any decision to make an application should be taken pragmatically and then actioned as per the relevant policies and procedures as referenced above.

4.2 Either authorisation for directed surveillance or for use of a Covert Human Intelligence Source (CHIS) may be required.

4.3 If in any doubt, the guiding principle is to refer to a line manager, with assistance from Legal Services, as necessary.

4.4 Reviewing open source sites does not require authorisation unless the review is carried out with some regularity.

4.5 Using social media for investigatory purposes, under statutory powers or otherwise, will meet the definition of **"directed surveillance"** if it is:

(1) covert;
(2) likely to reveal private information; and
(3) done with some regularity.

The primary consideration is then the privacy setting and whether the person being monitored has a public or private profile. A public profile will allow anyone to see information whereas with a private profile you have to be a friend of the person to see information about them.

4.6 A “one-off” is one on-line visit or a series of three or four visits that are closely connected in purpose, time and stage of the investigation. For example 3 visits within 2 weeks of each other could be a “one-off” if they relate to the same investigation and are closely related. However if there is a visit once a week for several weeks that would not be a “one-off” as it would appear to be monitoring the activity of the person.

4.7 It follows that there is no real difference between information from a social media source with public settings and a public website. A “one-off” piece of surveillance therefore would be outside the remit of the RIPA authorisation process.

4.8 For any surveillance that is more than a one-off those involved in considering whether to seek a RIPA authorisation should consider the parallel situation: live, covert observance of a person in public places.

4.8.1 A planned “one-off” drive-by, to establish a simple fact about a person, such as their place of abode, will also not require an authorisation, where there are no known other facts, such as a transaction occurring at the same time, likely to reveal private information.

4.8.2 If there are repeated observances, constituting more than a one-off, then the investigator should consider the real life, parallel situation and relate the use of internet to following a person, covertly, but in public. If an authorisation would be required in the real world, one would also be required in the virtual world.

4.9 Continued covert visits are likely to be unjustifiable without formal consideration under RIPA. Further surveillance by an investigating officer looking to obtain potential evidence requires a review of the need for authorisation with a line manager.

4.10 Further considerations for all will then include the reason for the surveillance and collateral information that may reasonably be suspected of being detected, as a precursor to a procedural application. Generally, the more necessary and proportionate the surveillance, the more likely that a formal application will be required.

4.11 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.”

4.12 If the application to join a site is a formality and there is no interaction with a suspect or their group, this will require a directed surveillance authorisation only.

4.13 The potential for a "relationship" to have been established or maintained must be considered formally with a line manager in such cases, obtaining advice from Legal Services as necessary.

4.14 Consideration must be given to the potential for the activity to constitute entrapment.

4.15 These rules apply to the use of any officer or agent of the council.

4.16 False identities are not unlawful, but real identities of others should not be adopted. However where there is need to penetrate someone's privacy settings, by be-friending them by using a false identity or pseudonym, this must be discussed with your manager and a RIPA authorisation will always be required. This can be equated to using a disguise to obtain information about a person, which is directed surveillance and would require RIPA authorisation.

4.17 If you engage in any form of relationship with the account operator then s/he becomes a CHIS and will require RIPA authorisation as well as management by a Controller and Handler with a record being kept and a risk assessment created.

5 WHAT ISN'T PERMITTED UNDER THIS POLICY

5.1 When it is discovered that an individual under investigation has set their social media account to private, officers should not attempt to circumvent those settings under any circumstances. Such attempts would include, but are not limited to;

- sending "friend" or "follow" requests to the individual,
- setting up or using bogus social media profiles in an attempt to gain access to the individual's private profile,
- contacting the individual through any form of instant messaging or chat function requesting access or information,
- asking family, friends, colleagues or any other third party to gain access on their behalf, or otherwise using the Social Media accounts of such people to gain access, or
- any other method which relies on the use of subterfuge or deception.

Officers should keep in mind that simply using profiles belonging to others, or indeed fake profiles, in order to carry out investigations does not provide them with any form of true anonymity. The location and identity of an officer carrying out a search can be easily traced through tracking of IP Addresses, and other electronic identifying markers.

5.2 Regardless of whether the social media profile belonging to a suspected offender is set to public or private, it should only ever be used for the purposes of evidence gathering. Interaction or conversation of any kind should be avoided at all costs, and at no stage should an officer seek to make contact with the individual through the medium of social media. Any contact that is made may lead to accusations of harassment or, where a level of deception is employed by the officer, entrapment, either of which would be detrimental and potentially fatal to any future prosecution that may be considered.

5.3 If an officer needs to carry out any of the above then this must be discussed with their manager and if necessary be approved by legal services and the Deputy Director of Community Protection before an RIPA authorisation is raised.

6 CAPTURING EVIDENCE

6.1 Once content available from an individual's social media profile has been identified as being relevant to the investigation being undertaken, it needs to be recorded and captured for the purposes of producing as evidence at any potential prosecution. Depending on the nature of the evidence, there are a number of ways in which this may be done.

6.2 Where evidence takes the form of a readable or otherwise observable content, such as text, status updates or photographs, it is acceptable for this to be copied directly from the site, or captured via a screenshot, onto a hard drive or some other form of storage device, and subsequently printed to a hard copy. The hard copy evidence should then be exhibited to a suitably prepared witness statement in the normal way.

6.3 Where evidence takes the form of audio or video content, then efforts should be made to download that content onto a hard drive or some other form of storage device such as a CD or DVD. Those CD's and/or DVD's should then be exhibited to a suitably prepared witness statement in the normal way. Any difficulties in downloading this kind of evidence should be brought to the attention of Serco who should be able to assist in capturing it.

6.4 When capturing evidence from an individual's public social media profile, steps should be taken to ensure that all relevant aspects of that evidence are recorded effectively. For example, when taking a screenshot of a person's social media profile, the officer doing so should make sure that the time and date are visible on the screenshot in order to prove when the evidence was captured. Likewise, if the evidence being captured is a specific status update or post published on the person's profile, steps should be taken to make sure that the date and time of that status update or post is visible within the screenshot. Without this information, the effectiveness of the evidence is potentially lost as it may not be admissible in court.

6.5 Due to the nature of social media, there is a significant risk of collateral damage in the form of other, innocent parties' information being inadvertently captured alongside that of the suspected offender's. When capturing evidence from a social media profile, steps should be taken to minimise this collateral damage either before capturing the evidence, or subsequently through redaction. This might be particularly prevalent on social media profiles promoting certain events, where users are encouraged to interact with each other by posting messages or on photographs where other users may be making comments.

7 General

7.1 Social media accounts must only be accessed on devices belonging to the council. If there is a need to access an account on one not belonging to the council this must be discussed and approved in writing by your manager.

7.2 A log must be kept of the use social media in any investigation detailing the reasons why it was necessary to use it, the results found and any collateral damage

to other parties.. This must be approved by your manager if it will be used in evidence.

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 to prove this is true. 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 the RIPA as it 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 would not be required as the employee is not committing a criminal offence. The HR department should take advice from legal services in such a case.

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, a directed surveillance RIPA authorisation must be considered. Full notes of the surveillance must be kept. If the officer then changes their account settings to private the manager should not send a friend request to the officer but should discuss the next steps with their manager as their might be other ways of obtaining the required information.

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 committed then RIPA cannot be used. RIPA cannot be used for civil action. It is unlikely that by looking at social media accounts the information required would be found. Other methods of obtaining the information should be used.

4. Officers seek to conduct directed surveillance against an individual on the grounds that this is necessary and proportionate for the collection of a tax as they have been claiming various housing and council tax rebates. They wish to monitor social media accounts on an ongoing basis to assist in the evidence gathering. The accounts have a public profile.

   Such surveillance could also result in the obtaining of some information about members of the individual's family, who are not the intended subjects of the surveillance. The authorising officer should consider the proportionality of this collateral intrusion, and whether sufficient measures are to be taken to limit it, when granting the authorisation. This may include not recording or retaining any material obtained through such collateral intrusion.

8 LEGISLATIVE OVERVIEW – LINKS

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

- Secretary of State and the Office of Surveillance Commissioners Guidance

https://osc.independent.gov.uk/

- 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