22/23 Annual Counter Fraud Report

Appendix G

Social Media Policy for Investigations

June 2023

Social Media Policy for Investigations

Page

Introduction

It is recognised that the use of the internet and, in particular, social media sites such as Facebook, Linked-in, Twitter, Snapchat, Instagram, etc. and other internet sites such as E-Bay can provide useful information for council staff carrying out investigations or gathering evidence. However, accessing an individual's or a company's internet and/or social media sites may potentially fall within the definition of covert directed surveillance, which would require a Regulation of Investigatory Powers Act 2000 (RIPA) authorisation and subsequent approval to be sought from a Magistrates' Court.

Failure to seek authorisation when necessary could result in the Council breaching an individual's right to privacy (Article 8 of the Human Rights Act 1998). It is therefore essential that investigating officers adhere to both this policy, and the Council's *Regulation of Investigatory Powers Act 2000 Corporate Authorisation Policy*, when considering accessing the internet and/or social media sites as part of an investigation or to gather evidence and intelligence.

Compliance to Data Protection Legislation (the Data Protection Act 2018 (DPA) and the General Data Protection Regulation (GDPR)) must also be considered and ensured throughout any investigation.

This policy should also be read in conjunction with the Home Office's statutory codes of practice for covert surveillance and for Covert Human Intelligence Source (CHIS).

What is social media?

Social media has become a significant part of many people's lives, with individuals regularly using and interacting with different forms of social media. By its nature, social media accumulates a considerable amount of information about an individual's life, from daily routines to specific events. Their accessibility on mobile devices can also mean that an individual's location at a given time may also be recorded when they interact with a form of social media on their devices.

The number and types of social media available to the public is constantly changing. In a given year, new sites may open whilst some of the more established sites could decrease in popularity.

Social media can therefore be a very useful tool when investigating alleged offences with a view to bringing a prosecution or taking other action. The use of information gathered from the various different forms of social media available can assist in substantiating or refuting information provided by a defendant, or an allegation made by a complainant.

However, not all information published on social media is true and care must be taken as to the validity of the information recorded on social media. Therefore, and if possible, it would be prudent to attempt to validate the information with another source of intelligence. The information obtained must only relate to the investigation being carried out and not for general "*fishing*". (The term "*fishing*" is used when the investigating officer reviews or obtains information that is not relevant to the investigation, for example, the investigation is relating to the illegal sub-letting of a Council property. However, the investigating officer starts looking at information relating to the page owner's family and friends.)

Social media encompasses a wide range of web-based services, which assist individuals or businesses to construct a public or semi-public profile, or to create a platform for sharing views or information. Typical characteristics can include:

- The ability to show a list of other users with whom the primary user shares a connection, often termed "*friends*" or "*followers*", and

- Hosting capabilities for audio, photographs and video content.

Current examples of social media sites include:

- Facebook
- Twitter
- Instagram
- LinkedIn
- Pinterest
- Google+
- Tumblr
- Flickr
- Reddit
- TikTok

The majority of social media services can allow its users to decide who can view their activity through the use of privacy settings, and individuals are able to set the level of information that can be viewed publically. Information that is publicly available is known as an individual's public profile. A public profile will allow anyone to see information that is contained on the webpage about the individual.

The opposite of a public profile is a private profile, where a user does not allow everyone to access and use their content, and one would usually have to be a "*friend*" of the individual (or page owner) to see information about them. However, for both public and private profiles, respect should still be shown to that individual's right to privacy under Article 8 of the Human Rights Act 1998.

Although 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 as giving authority to being monitored by the Council. The information is still the property of that individual.

When is a RIPA authorisation required?

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 sensibly and in line with the Council's *Regulation of Investigatory Powers Act 2000 Corporate Authorisation Policy*.

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

- Covert but not intrusive;
- Conducted for the purposes of a specific investigation or operation, and
- Likely to reveal private information.

Surveillance can involve the monitoring, observing or listening of individuals. This includes their movements, conversations, activities or other communications, or recording anything with a surveillance device. If a RIPA authorisation would be required ordinarily, then one would also be required in the virtual world. There is no difference between information from a social media source with public settings and a public website.

A RIPA authorisation relating to the use of social media provides safeguards for both the investigating officer and the Council if a claim is made under Article 8 of the Human Rights Act 1998 (Right to respect for private and family life).

For a criminal investigation, any evidence obtained contrary to the Council's *Regulation of Investigatory Powers Act 2000 Corporate Authorisation Policy* may be inadmissible, as well leaving scope for a civil action against the London Borough of Camden, including a complaint to the Investigatory Powers Tribunal. However, reviewing open source sites does not usually mean a RIPA authorisation is automatically required, unless the surveillance is conducted for a specific investigation and is likely to reveal private information. Factors to consider 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:
- 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), or
- 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.

There are some social media webpages where viewing their content can only be possible if it is first "*liked*" by the profile wishing to access it, for example, a Facebook group; a team account or "*team profile*" should be created for this purpose rather than creating one using a false identity. The "*team profile*" should clearly show that it is from the Council, for example, a Facebook group page is known to being used to discuss and sell counterfeit goods and Trading Standards would like access to its content, by showing that the "*like*" is from the Council, it confirms that the viewing is being made overtly by Trading Standards and therefore falls outside of RIPA rules; it could also act as a deterrent for the illegal activity to cease. A "*team profile*" could also assist the Housing Investigations Team, for example, in a similar way when receiving intelligence that an individual is advertising that their Council property is available to rent on social media.

For any covert surveillance that is more than a "*one-off*", a RIPA authorisation must be considered and either an authorisation for directed surveillance or for the use of a Covert Human Intelligence Source (CHIS) would be required. Consideration must also be given to the potential for the activity to be regarded as entrapment.

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. However, where there is need to apply online to join a platform this may require authorisation for the use of a CHIS but this would be dependent on the existence of a relationship.

If the investigating officer engages in any form of relationship with the account operator then a RIPA authorisation for the use of a CHIS is required, as well as management by a Controller and Handler, with a record being kept and a risk assessment created. Please refer to the Council's *Regulation of Investigatory Powers Act 2000 Corporate Authorisation Policy* for further guidance.

If in any doubt, the guiding principle is to refer to a line manager and/or seek advice from the Council's RIPA Co-ordinating Officer or RIPA Senior Responsible Officer (SRO), with assistance from Legal Services, as necessary.

What is not permitted?

When it is discovered that an individual under investigation has set their social media account to private, investigating officers should not attempt to circumvent those settings under any circumstances.

Although false identities are not unlawful, real identities of others should not be adopted, for example, the investigating officer should not befriend an individual by creating a profile in the name of someone they may know, i.e. a friend, relative or relative of a friend, etc. However, where there is need to penetrate an individual's privacy settings, by befriending 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 likened to using a disguise to obtain information about an individual, which is directed surveillance and therefore, would require RIPA authorisation.

Investigating officers should also keep in mind that simply using profiles belonging to others, or indeed fake profiles, in order to carry out investigations may not provide them with anonymity; the location and identity of an investigating officer carrying out a search could be traced through tracking of IP (Internet Provider) Addresses and/or other electronic identifying markers.

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, and at no stage should an investigating 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 investigating officer, entrapment; either of which would potentially compromise and be detrimental to any future prosecution that may be considered.

Below are a list of actions that investigating officers should not undertake:

- Sending "friend" or "follow" requests to an individual social media webpage;
- 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, or
- Asking family, friends, colleagues or any other third party to gain access on their behalf, or otherwise using the social media accounts of such individuals to gain access, or any other method which relies on the use of subterfuge or deception.

Record keeping

Once any content that is 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.

Where evidence takes the form of a readable or otherwise visible 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 s.9 witness statement in accordance with the Criminal Procedure and Investigations Act 1996 (CPIA).

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 CDs and/or DVDs should then be exhibited to a suitably prepared formal s.9 witness statement in accordance with CPIA.

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 an individual's social media profile, the investigating 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. Similarly, if the evidence being captured is a specific status update or post published on the individual's profile, steps should be taken to ensure 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.

Due to the nature of social media, there is a risk of collateral damage in the form of other innocent parties' information being inadvertently captured, alongside that of the subject of the investigation. 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.

Each investigation or enforcement team should record the accessing of any social media site or page on a central log in a spreadsheet and ensure that it captures the following information:

- Title of investigation
- Investigation case number
- Full URL (web address) of the webpage accessed
- Date and time the webpage was accessed
- Date and time the webpage was accessed previously
- Reason for accessing the webpage
- Investigating officer who accessed the webpage
- Manager authorising access
- What content was captured, e.g., text, photograph, audio, etc.
- Was RIPA authorisation required
- URN of RIPA authorisation
- RIPA authorisation expiry date

Where recorded material (in any form or media) is obtained during the course of an investigation that might be relevant to an investigation, or to pending or future civil or criminal proceedings, then it should not be destroyed but retained in accordance with the requirements of the Data Protection Act 2018, the Freedom of Information Act 2000, the Criminal Procedure and Investigations Act 1996, and any other legal requirements, including those of

confidentiality, and the Council's *Retention Schedule & Disposal Policy* and *Data Protection Policy*.

Summary of the process to be followed

Where an investigating officer considers it necessary to view a social media site to investigate an allegation or an individual, the process to be followed is:

- Before viewing any social media site, the investigating officer must seek the approval of their direct line manager.

- Social media sites should only be accessed on devices belonging to the Council. If there is a need to access an account on a device not belonging to the Council, this must be discussed and approved in writing by your line manager.

- Investigating officers must not use their own personal or private account when accessing social media sites for investigation and/or evidence gathering, only Council accounts should be used.

- Investigating officers may access the main page of an individual's profile to take an initial view as to whether there is any substance to the allegation of the matter being investigated. The initial viewing must be reasonable, for example, it would not be reasonable to spend any significant amount of time searching through various pages of an individual's profile or to print out several pages just in case they may reveal something useful.

- The Council should keep a log recording when social media sites are viewed for investigations and/or evidence gathering. Each single viewing of a company or individual's social media site must be recorded on the log. Each investigation or enforcement team should retain their own log and will be responsible for ensuring that it is recorded and maintained accurately.

- If it is considered that there is a need to monitor a company's or an individual's social media site, then the investigating officer must refer the matter back to their line manager for consideration as to whether a RIPA authorisation is required. If investigating officers are in any doubt as to whether an authorisation is required, they should seek advice from the Council's RIPA Co-ordinating Officer or RIPA SRO, with assistance from Legal Services, as necessary before continuing to access a social media site.

- These rules apply to all investigating officers or agents of the Council.

Appendix ends