Guidance on the Use of Social Media in Investigations

Version:	~~August 2022~~October 2024
Document Owners:	Group Head of Law & Governance~~Council Advice & Monitoring~~ (RIPA Senior Responsible Officer) ~~Internal Audit Manager~~
Approved By:	Audit & Governance Committee ~~Corporate Management Team~~

ARUN
DISTRICT COUNCIL

Background

The Council has an adopted approved Corporate Policy and Procedures ~~D~~document on the Regulation of Investigatory Powers Act 2000 (RIPA) ("the Policy"). The Policy sets out the legislative basis, definitions and the Council's procedures for authorising directed surveillance and the use of Covert Human Intelligence Sources under RIPA. The Policy also explains that the Council has produced a separate guide to the use of Social Media in investigations, and this document provides guidance to officers on how Social Media may and may not be used as part of an investigation, and the risks associated with the use of Social Media. ~~For all relevant bodies, RIPA arrangements and use fall under the oversight of the Investigatory Powers Commissioner's Office (IPCO), which assumed responsibility from the former Office of Surveillance Commissioners (OSC) in September 2017, and the Council may be subject to a periodic inspection to ensure that it complies with legislation and guidance.~~

~~Results and themes from inspections undertaken have been included in past Annual Report of the Chief Surveillance Commissioner to the Prime Minister and to the Scottish Ministers. In the reports for both 2013-14 and 2014-15, comment was raised on the use of social networks in investigations.~~

~~In respect of Social Networks the 2013-14 report stated:-~~

- ~~*"This is now a deeply embedded means of communication between people and one that public authorities can exploit for investigative purposes."*~~
- ~~*"Although there remains a significant debate as to how anything made publicly available in this medium can be considered private, my Commissioners remain of the view that the repeat viewing of individual 'open source' sites for the purpose of intelligence gathering and data collation should be considered within the context of the protection that RIPA affords to such activity."*~~
- ~~*"I strongly advise all public authorities empowered to use RIPA to have in place a corporate policy on the use of social media in investigations."*~~

~~The 2014-15 report reaffirmed this:-~~

- ~~*"Public authorities now make use of the wide availability of details about individuals, groups or locations that are provided on social networking sites and a myriad of other means of open communication between people using the Internet and their mobile communication devices."*~~
- ~~*I repeat my view that just because this material is out in the open, does not render it fair game. The Surveillance Commissioners have provided guidance that certain activities will require authorisation under RIPA and this includes repetitive viewing of what are deemed to be 'open source' sites for the purpose of intelligence gathering and data collation."*~~
- ~~*"My inspections have continued to find instances where social networking sites have been accessed, albeit with the right intentions for an investigative approach, without any corporate direction, oversight or regulation."*~~
- ~~*"This is a matter that every Senior Responsible Officer should ensure is addressed, lest activity is being undertaken that ought to be authorised, to ensure that the right to privacy and matters of collateral intrusion have been adequately considered and staff*~~

~~*are not placed at risk by their actions and to ensure that ensuing prosecutions are based upon admissible evidence."*~~

~~In August 2018, the Home Office issued its Revised Code of Practice covering Covert Surveillance and Property Interference and this now includes a section on 'online covert activity'.~~

This ~~corporate~~ guidance ~~document~~ has been developed to ~~cover~~ support the Council in this regard. For the purposes of this document, public domain or 'open source' information is defined as any Internet resource that is open and available to anyone.

This guidance must always be read in conjunction with the Policy.

While activity involving the use of social networks in an investigation may be deemed to be surveillance, within the meaning of RIPA (S.48(2)), not all will require a RIPA authorisation (or qualify for the protection offered through RIPA compliance). Depending upon the circumstances, the IPCO and the Home Office have advised that such activity could be classed as Covert Directed Surveillance or the use of a Confidential Human Intelligence Source (CHIS) on a case by case basis

1. Social Media and the Internet

Any officer considering internet / social media investigation of individuals must first consider the detailed guidance provided in the codes of practice and consult with their service manager and the RIPA Co-ordinating Officer.

1.1 The Internet can be a powerful tool supporting Council investigations – websites and social media allow ready access to information. As a public body, the Council needs to balance the power of the internet with our obligations to remain within the law.

1.2 Basic Principles

While it is possible to obtain significant information about individuals without leaving the office, the same principles apply as would in the case of information we might gather by following, photographing or filming individuals. Officers should view the internet in the same way as they would view information received directly from a complainant, a witness or a suspect in 'the real world'.

1.2.1 Initial Google Searches

A Google search for an individual may be thought of as an initial 'drive-by' observation in an investigation. It is broadly equivalent to an officer responding to an initial complaint or tip-off and visiting a particular location to establish 'the lay of the land'. It doesn't gather significant, detailed or private information, but

it is a starting point that allows us to decide if more detailed and directed investigation is required and / or possible.

An initial Google (or similar) search is not covert or directed surveillance and is unlikely to require RIPA authorisation.

Details of any such searches and their results should, however, be recorded in any notes or records of a given case.

1.2.2 Detailed Google Searches

While initial Google search results are equivalent to an initial drive-by in a case, if this is continued covertly and becomes a focussed search, likely to result in the obtaining of private information about a person or group the activity becomes 'directed' within the definition of Directed Surveillance. RIPA Council guidance.

A shift into the definition of Directed Surveillance is significantly more likely when an initial google search produces social media links for a person under investigation.

1.2.3 Social Media Information

An initial look on social media platforms such as Facebook, LinkedIn, Twitter and others can usually be viewed in the same way as an initial google search: that is, an officer is looking to see if a particular person has an online presence– the officer is simply looking to see if there are any resources that might provide lines of enquiry in future, more detailed, investigation.

However, returning to look at / into a person's online presence in more detail in order to monitor it or extract information relevant to an investigation is likely to require authorisation and advice must be taken on whether authorisation is required before proceeding.

Anyone cultivating an online relationship with an investigation subject (for example, a 'friend request' or similar) is likely to be moving into the scope of CHIS investigations, and advice must be taken on whether authorisation is required before proceeding.

~~**General RIPA Information**~~

~~The IPCO (ex-OSC) guidance is that:-~~

> ~~*"The Internet is a surveillance device as defined by RIPA section 48(1). Surveillance is covert 'if, and only if' it is conducted in a manner that is calculated to ensure that persons who are subject to the surveillance are unaware that it is, or may be, taking place.' Knowing that something is happening is not the same as an awareness that it is or may be taking place."*~~

While activity involving the use of social networks in an investigation may be deemed to be surveillance, within the meaning of RIPA (S.48(2)), not all will require a RIPA authorisation (or qualify for the protection offered through RIPA compliance). Depending upon the circumstances, the IPCO and the Home Office have advised that such activity could be classed as Covert Directed Surveillance or the use of a Confidential Human Intelligence Source (CHIS) on a case by case basis:-

- Covert Directed Surveillance means surveillance which is carried out in such a way that the person(s) subject to it is unaware that it is or may be taking place

  As a result of the Protection of Freedoms Act, from 1 November 2012 Directed Surveillance authorisations will have a crime threshold applied whereby local authorities can only authorise use of directed surveillance under RIPA to prevent or detect criminal offences that are either punishable, whether on summary conviction or indictment, by a maximum term of at least 6 months' imprisonment or are related to the underage sale of alcohol and tobacco.
- A person is a Covert Human Intelligence Source (CHIS) if they establish or maintain a relationship with another person in order to:-
  - covertly obtain information;
  - provide access to information to a third party; or
  - covertly disclose information obtained by the use of such a relationship and the other person is unaware that the purpose of the relationship is one of the above.

RIPA use now not only requires the internal approval of an Authorising Officer but also that of a magistrate. However, RIPA is permissive legislation, so failure to obtain appropriate authorisation does not render surveillance automatically unlawful. It could however lead to any evidence obtained being deemed inadmissible and/or civil action taken against the Council / Officers for breach of the subject's right to privacy under Article 8 of the European Convention on Human Rights.

The Convention qualifies this right so that in certain circumstances the Council may interfere in that person's right if that interference is:-

- in accordance with the law;
- necessary; and
- proportionate.

Investigation with Service areas which could potentially access social media for intelligence / information gathering in the course of their duties indicates that in most cases the actions being investigated would not meet the crime threshold. Guidance received is that where a proposed investigation does not relate to an activity that meets the above crime threshold for obtaining protection under RIPA, the Council should

~~follow the same processes for assessment, evidencing necessity / proportionality and internal Authorising Officer review (although without the involvement of a Magistrate), in order to provide a documented trail as a defence in the event of subsequent litigation.~~

~~RIPA is a complex piece of legislation. Reference should be made to the more detailed information, including explanations of necessity and proportionality, contained in the Council's RIPA policy, available via the intranet / Sharepoint.~~2.

Council Guidance

2.1 From the above, the Council's agreed guidance is that social networking is an acceptable tool which may be used in investigations / research. An investigation may be required e.g. where a post on social media is perceived as inappropriate (e.g. it is derogatory, insulting or damaging to the reputation of the Council, members of staff / Members or external parties) and brought to the attention of management by a member of staff or the public. However, such use must be subject to adequate consideration and authorisation(s) which will depend upon the activity being undertaken:-

- 2.1 ~~b~~Browsing (monitoring) 3rd party posts on social networking sites / feeds (e.g. Facebook ,Twitter, etc.) solely for the purposes of identifying comments (positive or negative) about the Council and its activities (as is also undertaken for newspapers) is a research activity and should need no additional RIPA consideration.

- 2.2 C~~c~~asual (one-off) examination of public posts on social networks as part of investigations undertaken is allowable with no additional RIPA consideration.

- 2.3 R~~r~~epetitive examination / monitoring of public posts as part of an investigation must be subject to assessment and may be classed as Directed Surveillance as defined by RIPA.

- 2.4 examination / use of any ostensibly 'private' mechanisms on social networks (e.g. as a 'friend' on Facebook, use of 'private' messaging facilities on Twitter, etc.):-
  - within an existing relationship where the parties are known to each other, but information that is freely obtained is used or passed on to an appropriate area for use in an investigation.
  - through a new relationship set up in an open manner (i.e. in the name of the Council).

  Must be subject to assessment and may be classed as either Directed Surveillance or the use of a CHIS under RIPA.

2.5 In any circumstances:-

- where a relationship is set up in a 'covert' manner specifically to obtain information
- a person known to the subject becomes a 'friend', etc. specifically for the purposes of the investigation
- a person becomes a 'friend', etc. in a false or misleading name
- where a dialogue is entered into in order to elicit information for the investigation with the subject remaining unaware (as this may be classed as entrapment)

Consideration MUST be given to obtaining appropriate authority under RIPA and this must consider whether it constitutes Directed Surveillance or the use of a CHIS.

2.6 On a case by case basis, consideration must be given to whether the investigation is into an activity that will require full RIPA authorisation (including Magistrate approval), or to follow a similar process for internal authorisation only, and appropriate documentation raised.

2.7 Under no circumstances should an investigating officer encourage inappropriate, fraudulent or criminal behaviour in order to provoke a response as part of the use of social networking facilities in ANY of the circumstances described above.

3. Corroborating Evidence

3.1 In using information obtained from the Internet / social networks, it must be recognised that the 'open source' environment is by nature insecure. Information obtained cannot be assumed to be fact and should therefore be subject to separate confirmation. Ideally, additional corroborating evidence should be obtained from a more robust source.

3.2 As part of the investigation, consideration must also be given to the circumstances of the case and whether the information is, in fact, demonstrating inappropriate activity. (For example, Facebook postings could suggest that a 'sick' employee is engaging in activity that is inconsistent with their condition – however, without additional medical advice, or independent examination, this cannot be assumed as being the case). While such information may be introduced into investigative / disciplinary proceedings as potential evidence, it cannot on its own be deemed to be proof in support of an accusation.

4. Other Considerations

4.1 When considering the use of social networks in the conduct of an investigation, there may be a requirement for a risk assessment to be undertaken. This should include any Officers involved in the investigation (and potentially,

members of the public if information has been provided by them). Considerations should include:-

- whether the identity of the provider of 'private' information could become apparent to the subject of the investigation
- whether the activity involves the use of a CHIS.

~~***Further information on these requirements is contained in the Council's RIPA policy, available via the intranet / Sharepoint.***~~

4.2 In order to ensure that rights are respected, the General Data Protection Regulation / Data Protection Act 2018 must also be complied with.

4.3 Any investigation must be conducted, documented and evidence obtained / secured following proper Council procedures and meeting any appropriate legislative requirements.

4.4 Where the subject of online surveillance is (or includes) an employee then the Information Commissioner's Office (ICO) Employment Practices Code (part 3) will apply. This requires an impact assessment to be done before the surveillance is undertaken to consider, amongst other things, necessity, proportionality and collateral intrusion.

~~The Council's Internet & E-Mail Acceptable Usage Agreement (issued to all staff) covers the expected behaviours the Council requires in respect of the use of corporate information systems and advises that inappropriate use could lead to disciplinary action. It should be noted that it also contains the following statement:-~~

> ~~*Where personal social media accounts are used by employees (e.g. Facebook, Twitter, etc.), whether at approved times during the business day or in non-work time, the Council expects the same usage standards to apply particularly with regard to statements or comments regarding the Council, its employees or its Members, which may be read by members of the public or other staff.*~~

~~In the event it is brought to the attention of management that these standards have not been applied, the Council may investigate the matter in line with appropriate corporate policies. Should an investigation involving an employee result in disciplinary action, then it is important that the correct disciplinary procedures are followed. Should there be subsequent referral to a tribunal, then the key factor in any disciplinary situation is for the employer to have acted fairly and "within the range of reasonable responses". It will not be enough for an employer to simply argue that the employee has breached its social media policy. A tribunal will look at the wider circumstances and many competing factors when deciding on the reasonableness of a disciplinary decision.~~

~~**Advice To Officers**~~

~~As noted elsewhere in this guidance document, there remain some grey areas over the legitimate use of social networking in investigations and the IPCO themselves have recognised that "there is a fine line between general observation, systematic~~

~~observation and research." There is also the additional consideration as to whether an activity will meet the requirements for RIPA authorisation / the protection it offers or whether it must be conducted outside of this.~~

If an Officer is considering the use of social networking for such activity, or is uncertain as to how to proceed, then further advice on the guidance and the potential RIPA requirements may be obtained from:-

- RIPA Authorising Officers (~~the members of the Corporate Management Team~~listed within the Policy)
- Group Head of Law & Governance.~~Council Advice & Monitoring~~
- ~~Internal Audit Manager.~~

Associated Documents

This guidance is linked to a number of other Council documents which are available to staff via the Council's website and/or intranet (Sharepoint) site:-

- Corporate Policy and Procedures Document on the Regulation of Investigatory Powers Act 2000 (RIPA)
- Social Media Guidance for Councillors
- Social Media Policy & Guidance
- Internet & E-Mail Acceptable Usage Agreement
- Disciplinary Procedure.

Further information

- Further information on RIPA and the Home Office Codes of Practice may be obtained from the GOV.UK website:-
  https://www.gov.uk/government/publications/regulation-of-investigatory-powers-act-2000-ripa
  https://www.gov.uk/government/collections/ripa-codes
- Further information on the IPCO may be obtained from the Investigatory Powers Commissioner's Office website:-
  https://www.ipco.org.uk/
- Further information on Human Resources activity (including use in recruitment, disciplinary / grievance aspects, etc.) may be obtained from the ACAS website, covering Social Media in the Workplace:-
  http://www.acas.org.uk/index.aspx?articleid=3375
- Further information on the ICO Employment Practices Code may be obtained from the Information Commissioner's Office website:-
  https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf