SWLFP
South West London Fraud Partnership

Using Social Media in Investigations

Social Media has opened up numerous opportunities and is a key component to profiling the subject of an investigation. Twitter, Facebook, LinkedIn to name but a few have embedded themselves in people's lives. Posting to walls, tweets, video and image updates are emerging as a new trove of intelligence. Social media evidence can be a valuable addition to an investigation, revealing the kind of information that, years ago, would have been difficult, if not impossible, to find. But it has to be gathered in a way that will hold up in court. Because it's such a new source of evidence in investigations, case law is developing rapidly.

In using social media sites for investigative purposes, it is vital that we do so lawfully. Listed below are six considerations that should be taken into account when using social media for investigative purposes (Source: CIPFA).

1. There can be no doubt many social media users are living their private lives in public. Article 8 of The Human Rights Act states everyone has a right to respect for their private life, their family, their relationships with others, and their correspondence (communications with others). Their privacy can only be interfered with if legitimate purposes and certain conditions apply – and then the interference must be necessary and proportionate and not excessive. It is too easy for an organisation to breach Section 6 of the Human Rights Act and act unlawfully.

2. Images of living persons and personal information is data regulated by the Data Protection Act. Collecting, processing, and storing this information from social media requires strict adherence to the Data Protection Act and associated Information Commissioner Guidance.

3. Regular monitoring, viewing, re-visiting of social media amounts to surveillance, which might be covert or overt, and require adherence to the Data Protection Act and the Regulation of Investigatory Powers Act if your organisation is a designated authority.

4. Those researching social media often don't find the information that is available, conducting scant Google or keyword searches, and not using the full potential of various search tools such the Advanced Search tools, Graph Search, Pages, Emotions, Wildcards, tagging and other Metadata and Geo-tagging data. The information obtained is not further developed using other open source internet resources.

5. Information obtained must be evaluated objectively. Who is actually saying this? How do they know this? Can the information be relied upon? Can the information be used as evidence?

6. Information captured from social media and used as evidence must be captured, stored and produced in accordance with accepted best practice. If it is not – then the evidence might not be accepted at a trial or hearing.

What is social media?

Social media describes websites that provide user-generated content. Whilst traditional media is controlled by editors, social media allows users to dictate the agenda.

Private Information

Private Information is information relating to a person's private or family life. It can include any aspect of a person's relationships with others, including professional or business relationships.

A person may have a reduced expectation of privacy when in a public place. But covert surveillance of their activities in public may still result in the obtaining of private information.

The Human Rights Act 1998 / European Convention on Human Rights, Article 8 provides that:

8.1 Everyone has the right to respect for his private and family life, his home and his correspondence.

8.2 There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals or for the protection of the rights and freedoms of others.

These principles apply equally to the online world, including social media sites; where access controls set by the owner of the information may be a determining factor in considering whether information posted on the internet is publicly available. or whether, by applying the access controls, the owner has removed the information from a wholly public space to a more private space where the information could be considered private.

Accessing social media to support an investigation

Information available via the internet may be required either prior to and/or during an investigation, however repeatedly accessing and recording such information may amount to directed surveillance.

When you intend to use the internet as part of an investigation, you must first consider whether the proposed activity is likely to interfere with a person's Article 8 rights. As a rule, directed surveillance should be the choice of last resort. Any activity

likely to interfere with an individual's Article 8 rights should only be used when necessary and proportionate to meet the objectives of a specific case.

When considering accessing social media investigators must:

- Obtain approval from their line manager (see Appendix A - Social Media Authorisation Requests).
- NOT use their own private accounts to view the social networking accounts of other individuals (we have a SWLFP Facebook account).
- NOT "friend" individuals on social networks as doing so openly could put you at risk. If you believe that you need to communicate covertly online, for example contacting individuals using social media websites, the need for a CHIS authorisation must be considered.
- In viewing an individual's profile on a social networking site should do so only to obtain evidence to support or refute their investigation as further viewing of open profiles on social media networking sites to gather evidence could amount to surveillance and the need for authorisation under RIPA must be considered if further monitoring of an individuals status is to take place.
- Be aware of the importance of the need to verify the accuracy of information on social networking sites if such information is to be used as evidence, as individuals may post information that inflates, exaggerates or embellishes the truth.
- Once approval to access social media information in support of an investigation has been obtained evidence must be gathered in a way that is legal and useful (see Appendix B - Enquiry Record Log).

Extracts from ACPO Good Practice Guide for Digital Evidence, Version 5 (October 2011)

When carrying out any evidence recovery it is essential that an audit trail of all activity carried out by the investigator is recorded in a log. The recommended method for copying a website is to visit the site and record the relevant pages using video capture software so there is a visible representation of how they look when visited at the time. If video capture software is not available then the pages can be saved as screenshots. It is also advisable to follow this by capturing the web pages themselves either by using website copying software or saving the individual pages. Copying the pages themselves, as well as obtaining a visual record, means that the code from the web pages is also secured should that become relevant later.

Anyone visiting a website generally exposes a certain amount of information to the website, for example it is common on police systems to have a web browser which is branded with the forces name. This branding is exposed to a website being visited and so may be recorded in logs on the site along with other information amongst which, will include the pages visited.

If it appears likely that the evidence on the website might be lost by a delay in carrying out the above procedures then the person reporting may be asked to make a copy of the evidence by whatever means they are capable of (either printing, screenshot or saving pages), alternatively this could be done by the person receiving the report. Before taking these steps every effort should be made to secure the services of a competent person to carry out this work as failing to capture the information correctly could have a detrimental impact on the investigation.

Where there is difficulty in capturing the evidence by visiting the site it might be possible to make an official request to the owner of the site by whatever legal procedures are required within the jurisdiction. The CSP/ISP SPOC or Digital Forensic Unit can usually advise on the appropriate procedures.

By making a request to the service provider hosting the site it may be possible to recover evidence of who has created the web page or posting. It is not unusual for details of the user such as name, address, phone number, banking details, email address, and alternative email address to be recorded by a host.

If there is a requirement to identify who has committed some activity on a website, for example where a fraud has been committed by purchasing goods from a website or by posting a message on a website, the likelihood is that the suspect may be traceable from logs on the site. When any user accesses the Internet they are allocated a unique address known as an IP address and their Internet Service Provider (ISP) keeps logs of the times and dates and the identity of the user allocated any IP address.

When a user visits a site and conducts some activity, for example logs on, posts a message, or makes a purchase, it is likely that the user's IP address has been logged by the website. It is often possible to obtain copies of logs from websites if there is a requirement to see who has been active on a website by making a request via the force CSP/ISP SPOC.

If the evidence is no longer available to be retrieved by any of the above means, and where the use of resources can be justified by the seriousness of the case, it may be possible to recover evidence of the site contents from an end user device that has been used to view the site by conducting a forensic examination of the device.

Investigating - Key Points

- Ensure manager/service manager approval before researching websites, forums and blogs for specific investigations.
- Do not change original data.
- Competent persons are to be used to access data.
- Audit trail of all actions in relation to original data to be recorded. Should provide sufficient detail so that a 3rd party can follow and achieve the same result.

- The lead investigator has responsibility for ensuring the law and these principles are adhered to.
- Repeated visits to websites, forums and blogs are likely to amount to Directed Surveillance and a RIPA authority will be required.

Collection of Evidence – Key Points

- Use trained staff
- Maintain log of activity
- Save web page address to disk (master exhibit)
- Save screen shots of relevant pages to disk (master exhibit)

Key Legislation

- Human Rights Act 1998 / European Convention on Human Rights
- Regulation of Investigatory Powers Act 2000
  Part I – Interception of Communications and the Acquisition of Communications Data
  Part II – Surveillance and Covert Human Intelligence Sources
- Computer Misuse Act 1990
- Data Protection Act 1998
- Criminal Procedures and Investigations Act 1996

Comments from the Office of Surveillance Commissioners

"Many local authorities have not kept pace with these developments. 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."