ASSOCIATION OF CHIEF POLICE OFFICERS

Online Research and Investigation

This document is intended to provide guidance to police officers or staff engaged in research and investigation across the internet.

This guidance is not a source of law but is subject to the legislation and to the statutory Codes of Practice.

It is being circulated in the interests of promoting good practice and consistency across law enforcement.

If you would like any advice regarding the guidance provided in this document please contact the ACPO preferred source of advice at the NCA Specialist Operations Centre on 0845 000 5463

Foreword by ACPO leads

This ACPO Guidance for Online Research and Investigation together with the Examples Supplement is provided to assist staff engaged in research and investigations that require the use of the internet. The document is circulated to promote good and consistent practices across law enforcement agencies. There is currently a variety of approaches by forces and agencies in the way such activity is conducted. This guidance is the result of lengthy consultation and legal advice, it is a collaboration between the ACPO leads for Open Source, Undercover and RIPA.

This document must be considered together with the Chief Surveillance Commissioner's Procedures and Guidance document (2011) as amended.

It is important to emphasise that whether or not any authorisation is required by a law enforcement agency will depend on the precise circumstances of any particular case.

We commend the guidance to you.

Chief Constable Steve Kavanagh
ACPO Open Source lead

Commander Richard Martin
ACPO Undercover lead

ACC Jon Boutcher
ACPO RIPA lead

Contents

Introduction

This guidance focuses on how the principles set out in legislation apply to the use of the internet, including social media, as an investigative tool. It does not replace statutory guidance. Each activity should be considered on a case by case basis, in line with your force or agency policies on engagement, communications and use of technology.

Covert investigative techniques likely to interfere with a person's Article 8 rights should be used only when necessary and proportionate. Both the Regulation of Investigatory Powers Act (RIPA) and the Data Protection Act (DPA) provide a framework for ensuring that such action is lawful and in accordance with the European Convention of Human Rights (ECHR) and the Human Rights Act (HRA). RIPA Codes of Practice provide statutory guidance on the use of some of these techniques.

The document is subject to continuing review and amendment to take account of developments in legislation, technology, the effect of legal judgments and stated cases. Subsequent versions will be available on POLKA.

Online research and investigation is a powerful tool against crime. It also presents new challenges to law enforcement as the use of such a tool can still interfere with a person's right to respect for their private and family life which is enshrined in Article 8 of the Human Right Act 1998 and ECHR.

Public authorities must ensure that any interference with this right is:

- necessary for a specific and legitimate objective – such as preventing or detecting crime;
- proportionate to the objective in question;
- in accordance with the law.

Whenever you are using the internet to gather intelligence or evidence you must consider whether you are likely to interfere with a person's right to respect for their private and family life and, if so, whether you should seek authorisation under RIPA for your conduct. The principles in this guidance have been prepared to help you identify if such authorisation is appropriate.

It is also essential to consider the effect of any collateral intrusion on the private and family life of other people not directly connected with the subject of the research or investigation.

Case by case judgement is vital when researching or investigating online.

Guiding Principles – Overview and operational risk considerations

Overview

- Online communication via the internet has, in recent years, become the preferred method of communication with other individuals, within social groups or with anyone in the world with internet access. Such communication may involve web sites, social networks (e.g. Facebook), chat rooms, information networks (e.g. Twitter) and/or web based electronic mail.

- Just because other people may also be able to see it, does not necessarily mean that a person has no expectation of privacy in relation to information posted on the internet. Using covert techniques to observe, monitor and obtain private information can amount to an interference with a person's right to respect for their private and family life. Authorisation regimes, such as RIPA, must be considered although RIPA is not the only legislation which can render such an interference lawful.

Operational Risk Considerations

- Any online research and investigation leaves a trace or 'footprint'. An operational decision will therefore need to be made as to whether you wish to ensure that your research is non-attributable i.e. cannot be traced back to law enforcement or to identifiable individuals, or whether you are happy for it to be attributable i.e. capable of being traced back to law enforcement.

- Non-attributable research and investigation must be carried out on equipment that cannot be attributed to law enforcement or identifiable individuals, just as attributable research and investigation must be carried out on attributable equipment. Carrying out any attributable activity on non-attributable equipment runs the risk of compromising the equipment and any operational activity which has been conducted on it.

- It is recommended that attributable research and investigation is restricted to publicly accessible search areas e.g. maps, street views, local authority sites, auction sites, etc and websites which have no requirement to register details in order to gain access.

- It is acknowledged that many officers and staff will have considerable experience of using the internet for their own personal online research. However managers should ensure that staff carrying out online research and investigation for law enforcement are both competent and appropriately trained.

Guiding Principles - Security ground rules

Always be aware of your force or agency security ground rules

Your organisation should have policies for handling online research and investigation. These should include such matters as:

The appropriate sourcing of equipment procured for covert use.

The separation of equipment used for covert and overt activity.

Ensuring that equipment used for covert activity cannot be attributed to law enforcement.

How and where to fully capture, record and retain information obtained online.

How and where to record the actions of the person conducting the research or investigation so that it is subsequently auditable.

The preferred methods of producing intelligence in an evidential format.

Guiding Principles – Use of a false persona

It is recognised that there will, for covert online research and investigation, be a requirement to create and use false persona accounts to gather information. The creation of a false persona for the purposes of online research and investigation does not, in itself, require authorisation under RIPA. It may, however, breach the terms and conditions of some sites, particularly social networks.

The use of a false persona in relation to a covert investigation may require authorisation under RIPA dependant upon the activity planned to be undertaken.

False personas should only be used for covert research and investigations which must be undertaken using a non-attributable computer.

The creation of a false persona should be agreed by a Detective Inspector (Intelligence or Covert Policing) or equivalent. Each agency should maintain a register of all such profiles created and used in the force/agency. This register should be maintained centrally and periodically reviewed taking into account the necessity and proportionality of maintaining and using each registered persona.

A log, recording the time, date, user and the policing purpose, should be maintained for each use of a false persona.

Guiding Principles – Open source

- Most of the information available on the internet is available to any person with internet access, either freely or for payment. Such information is widely known as open source information.
- Viewing open source information, either by attributable or non-attributable means, does not amount to obtaining private information because that information is publicly available. This is therefore unlikely to require authorisation under RIPA whether it is done on a one off basis or by repeated viewing.
- Recording, storing and using open source information in order to build up a profile of a person or a group of people must be both necessary and proportionate and, to ensure that any resultant interference with a person's Article 8 right to respect for their private and family life is lawful, it must be retained and processed in accordance with the principles of the Data Protection Act 1998.

Definitions

In relation to open source material ACPO provide the following definitions which may assist those involved in online research and investigation:

- Open Source Research - The collection, evaluation and analysis of materials from sources available to the public, whether on payment or otherwise, to use as intelligence or evidence within investigations.
- Open Source Information - Publicly available information (i.e. any member of the public could lawfully obtain the information by request or observation). It includes books, journals, TV and radio broadcasts, newswires, internet WWW and newsgroups, mapping, imagery, photographs, commercial subscription databases and grey literature (conference proceedings and institute reports).

Guiding Principles – Restricted access information

- Access to some of the information on the internet is restricted by its “owner”. A common form of such restriction is in social networks where a profile owner may use the privacy settings to restrict access to online “friends”.
- Viewing restricted access information covertly, will generally constitute covert surveillance and, as the information is not publicly available, it is likely that private information will be obtained. Authorisation as directed surveillance should be sought in these circumstances.
- Recording, storing and using restricted access information, in order to build up a profile of a person or a group of people must be both necessary and proportionate, and it must be retained and processed in accordance with the principles of the Data Protection Act 1998.
- The initial interaction involved in the act of bypassing privacy controls (the sending and acceptance of a friends request) may be minimal. In many cases it is considered unlikely that this, by itself, will meet the RIPA definition of a “relationship” and will not require authorisation as a Covert Human Intelligence Source (CHIS). However, much work may have had to be conducted to get to that stage without arousing suspicion. In addition, it may be difficult to predict how or at what pace that “relationship” will need to develop. If it is intended or considered likely that direct one to one interaction with another person will go beyond the initial request/acceptance it will be appropriate to seek authorisation as a CHIS. The creation of a false persona involving other “friends”, which are also false, in order to effect the deception and secure the information effectively amounts to “legend building” in support of the CHIS

Guiding Principles – Restricted access information

- Considerations of the potential for any subsequent interaction, that would qualify as a “relationship”, should be appropriately documented as part of the decision making process. This should include the reasons for any decision not to authorise the use of the undercover online operative undertaking the activity as a CHIS and contingency provisions for authorisation if subsequently considered appropriate.
- Although this minimal initial interaction will not require authorisation as a CHIS it is considered good practice for friends requests to be sent by a trained undercover online operative.

The Law - Overview

Online research and investigation techniques may impact on all or any of the following:

- 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
- Police Act 1997 Part III
- Computer Misuse Act 1990
- Data Protection Act 1998

Human Rights Act / European Convention on Human Rights

Both of these provide a number of fundamental rights which are central to all actions of law enforcement.

The right most likely to be engaged by officers and staff undertaking online research and investigation is Article 8 which states:

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.

Ensuring that RIPA authorisations are sought, where necessary, and that the material obtained is retained and processed in accordance with the provisions of the Data Protection Act should provide the lawful authority required by Article 8.2 for any perceived interference with Article 8.1.

Interception and Communications Data under RIPA

Interception of Communications

Part I Chapter I of RIPA regulates the interception of communications in the course of transmission by post or by a public or private telecommunication system.

Examples of such communications which those undertaking online research and investigation are likely to encounter may include, web based email and social network personal messages.

RIPA allows for interception by authority of a warrant signed personally by the Secretary of State. Material obtained by this means cannot be used in evidence.

RIPA also makes provision for the lawful interception of communications on certain conditions including: Where both sender and intended recipient consent (RIPA s3.1); Where one party consents and a directed surveillance authorisation is in place (RIPA s3.2); where, in relation to stored communications, another statutory power to obtain information is exercised RIPA s1(5)(c). Material obtained by these means can be used in evidence.

Definition of interception

Under section 2(2) of RIPA, interception of a telecommunication occurs by:

- modifying or interfering with the system or its operation; or
- monitoring transmissions made by the system; or
- monitoring wireless telegraphy transmissions to or from the system;

so as to make some or all of the contents of the communications available, while being transmitted, to a person other than the sender or intended recipient of the communication.

Note – The interception of a communication in the course of its transmission may, unless it is made lawful by one of the provisions in the previous column, constitute a criminal offence. Material obtained by means of an unlawful interception is not admissible in evidence.

Communications Data (CD)

Part I Chapter II of RIPA deals with the acquisition and disclosure of CD, which is everything but the content of the communications.

Online research and investigation may , for example, result in a requirement to attribute a telephone number to a subscriber or investigators may wish to identify the user of an internet protocol address of a device identified as accessing indecent images of children. Such data is classed as communications data and can be requested from service providers using the authorisation procedure under Pt I Chapter II.

Applications for communications data should be routed through the force's Single Point of Contact, a trained technical expert who will be able to advise on what is likely to be available, where it is likely to be and the most appropriate method of lawfully acquiring it.

Directed Surveillance and CHIS under RIPA

Directed Surveillance

Under section 26(2) of RIPA, surveillance is 'directed' if it is covert but not intrusive and is undertaken

- for the purposes of a specific investigation or a specific operation; and
- is likely to result in the obtaining of private information about a person; and
- is otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation under RIPA Part II to be sought for the carrying out of the surveillance.

As can be seen from the guiding principles described on pages 8 to 10 of this document, the likelihood of obtaining private information will be a determining factor when considering whether authorisation as directed surveillance is appropriate.

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.

This principle applies 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. Unrestricted open source information is unlikely to fall within the definition of private information.

Covert Human Intelligence Source (CHIS)

Under section 26(8) of RIPA, a person is a CHIS if he establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything below:

- he covertly uses such a relationship to obtain information or to provide access to any information to another person; or
- he covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

As can be seen from the guiding principles on pages 9/10 of this document, although the making and acceptance of a friends request constitutes some interaction with a person, it is minimal and is unlikely to satisfy the definition of a relationship. Authorisation as a CHIS need only be sought when it is anticipated that the relationship will be developed beyond this initial contact.

Property Interference under Pt III of the Police Act 1997

Touching or interfering with the property of another person, without their consent, constitutes an unlawful trespass and may possibly constitute criminal damage.

Where this is considered both necessary and proportionate for the prevention or detection of serious crime, Pt III of the Police Act 1997 provides for an authorisation to be sought for the interference.

This authorisation, generally given by a Chief Constable, is subject to oversight and in some circumstances, prior approval, by the Surveillance Commissioners.

Officers and staff conducting online research and investigation should be aware that property interference authorisation should be sought for such actions as:

- The examination (generally covert) of computers or other end user devices which have not been formally seized under a statutory power of seizure (e.g. Police and Criminal Evidence Act 1984).
- Using a password without the consent of the person with possessory rights, to gain entry to a computer.
- Covertly installing monitoring software.

It must be noted that, with few exceptions, Authorising Officers can only authorise property interference that will take place within their own relevant area. In the case of police forces this is their own force area or the area of any formal collaboration agreement of which they are part. Authorisation which purports to authorise interference outside the relevant area may render the force open to civil action. This is particularly relevant where the interference is done remotely.

Computer Misuse Act 1990

Sections 1-3 of the Computer Misuse Act 1990 introduced three criminal offences:

- unauthorised access to computer material;
- unauthorised access with intent to commit or facilitate commission of further offences; and
- unauthorised modification of computer material.

The basic offence is to attempt or achieve access to a computer or the data it stores, by inducing a computer to perform any function with intent to secure access. The precondition to liability is to be aware that the access attempted is unauthorised. Thus the following activities may constitute the offence :

- to use another person's username and password without lawful authority or consent to access data or a program;
- to alter, delete, copy or move a program or data;
- to impersonate that other person using e-mail, on line chat or other web based services.

A properly worded authorisation for property interference under Pt III Police Act 1997 may render lawful the first two of the above examples. However in cases where the interference is to be done remotely please see page 15 in relation to the authorisation of interference outside the Authorising Officer's relevant area.
A properly worded authorisation as a Covert Human Intelligence Source under Pt II RIPA 2000 may render lawful the third example.

Retention and processing of information.

Data Protection Act 1998 and other relevant legislation / guidance

The Data Protection Act 1998 deals with how material obtained must be handled. The DPA guiding principles are that personal data must be processed fairly and lawfully, must not be processed in a manner that is not compatible with the purpose for which it was obtained, must be relevant and adequate but not excessive and must not be kept longer than is required.

Much of the information gathered by online research and investigation will meet the definition of personal data. Case law has established that the processing of personal data is capable of interfering with a person's Article 8 right to respect for their private and family life, irrespective of whether the information was obtained under the authority of RIPA or otherwise.

The 2005 Code of Practice on the Management of Police Information (MoPI) states that Chief Officers have a duty to obtain information for police purposes (protecting life and property, preserving order, preventing the commission of offences, bringing offenders to justice, other duties and responsibilities of the police arising from common or statute law). For any interference with a person's Article 8 rights resulting from the processing of such information to be in accordance with the law, as required by Article 8.2, it is therefore essential that all information so obtained is processed in accordance with the principles of the Data Protection Act.

Previous ACPO guidance on MoPI was decommissioned in October 2012 and the content of this guidance was incorporated into Authorised Professional Practice (APP) - Information Management. APP can be accessed via the Police Online Knowledge Area (POLKA). POLKA is available to anyone connected to the Police National Network (PNN) and selected users of the Government Secure Intranet (GSI). If there are any difficulties accessing this information please contact the NCA Specialist Operations Centre on 0845 000 5463.

The retention of material obtained in a criminal investigation is also subject to the provisions of the Criminal Procedure and Investigations Act 1996 and its associated Code of Practice. This Act sets out a number of statutory criteria for the handling and retention of such material.

Chief Surveillance Commissioner's Views

Extract from OSC 2011 guidance, as amended.

Covert surveillance of Social Networking Sites (SNS)

308 The fact that digital investigation is routine or easy to conduct does not reduce the need for authorisation. Care must be taken to understand how the SNS being used works. Authorising officers must not be tempted to assume that one service provider is the same as another or that the services provided by a single provider are the same.

308.1 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.

308.2 Providing there is no warrant authorising interception in accordance with section 48(4) of the 2000 Act, if it is necessary and proportionate for a public authority to breach covertly access controls, 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 by a member of a public authority or by a person acting on its behalf (i.e. the activity is more than mere reading of the site's content).

308.3 It is not unlawful for a member of a public authority to set up a false identity but it is inadvisable for a member of a public authority to do so for a covert purpose without authorisation. Using photographs of other persons without their permission to support the false identity infringes other laws.

308.4 A member of a public authority 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 consent of the person whose identity is used, and without considering the protection of that person. The consent must be explicit (i.e. the person from whom consent is sought must agree (preferably in writing) what is and is not to be done).