NPCC Guidance on Open Source Investigation/Research

The National Police Chief's Council have agreed to this guidance being circulated to, and adopted by, Police Forces in England and Wales.

It is RESTRICTED under the Government Protective Marking Scheme and it is not disclosable under the Freedom of Information Act 2000.

Document information

Protective marking	**RESTRICTED**
Author	**Jennifer Housego**
Force/Organisation	**Kent and Essex Police**
ACPO Business Area	**Crime, Intelligence, Open Source**
Contact details	[redacted]
Review date	**April 2016**
Version	**April 2015**

This Guidance has been produced by the NPCC Intelligence Portfolio and has been endorsed by Chief Constables' Council on (date]. NPCC has agreed to this guidance being circulated to and adopted by Police Forces in England and Wales. It will be updated according to legislative and policy changes and re-published as required.

Any queries relating to this document should be directed to the author detailed above.

Contents

1. Aims

This document is intended to provide guidance to Police officers and staff using Open Source for intelligence and investigation.

It is based on current practice developed within the Metropolitan and other police forces.[1]

Definition of 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'.

1.1 Open Source Information

'Open Source is defined as publicly available information (i.e. any member of the public could lawfully obtain the information by request or observation). It includes books, newspapers, journals, TV and radio broadcasts, newswires, Internet WWW and newsgroups, mapping, imagery, photographs, commercial subscription databases and grey literature (conference proceedings and institute reports).

1.2 For the purposes of this policy it is recognised that commercial subscription databases may contain mixed data some of which is not available to the public but within the terms of the policy they are still considered open source. [redacted]

This document provides minimum standards and should be read and applied in conjunction with local force policy. This document and force policy should be adopted by all persons engaged in open source investigation/research (OSIR) in order to maintain the integrity of any evidence gained and in order to avoid compromise of the following:

- The hardware/software infrastructure of police computer systems
- Police tactics
- Ongoing and future police operations
- The personal safety of individuals
- Reputational risks to the organisation

NCALT e-learning packages are available to assist in understanding of the issues involved.

- Management of Police Information - Levels 1 – 4
- Communications Data in Investigations
- Introduction to Communications Data and Cybercrime.
- Open Source Intelligence Research – Level 1

2. LEGISLATION

Prior to engaging in any open source investigation/research staff should have a good understanding of the Legislation and Guidance that may apply, including:

[1] Includes NPCC RIPA in the modern world conference – March 2013

- Human Rights Act 1998 (HRA)
- Regulation of Investigatory Powers Act 2000 (RIPA)
- Computer Misuse Act 1980 (CMA)
- Data Protection Act 1998 (DPA)
- PACE 1984
- Criminal Procedure and Investigations Act 1996 (CPIA)
- Police Act 1997
- Management of Police Information 2010 (MoPI)
- ACPO principles for recovery of digital / computer data

Officers will also benefit from reading the 2015 Anderson Report – 'A question of Trust', as well as the 2015 report from the Royal United Services Institute entitled - 'A democratic Licence to Operate', which contains 10 tests of privacy below:

RUSI - Ten Tests for the Intrusion of Privacy

1. **Rule of law**: All intrusion into privacy must be in accordance with law through Processes that can be meaningfully assessed against clear and open legislation, and only for purposes laid down by law.
2. **Necessity**: All intrusion must be justified as necessary in relation to explicit tasks and missions assigned to government agencies in accordance with their duly democratic processes, and there should be no other practicable means of achieving the objective.
3. **Proportionality**: Intrusion must be judged as proportionate to the advantages gained, not just in cost or resource terms but also through a judgement that the degree of intrusion is matched by the seriousness of the harm to be prevented.
4. **Restraint**: It should never become routine for the state to intrude into the lives of its citizens. It must be reluctant to do so, restrained in the powers it chooses to use, and properly authorised when it deems it necessary to intrude.
5. **Effective oversight**: An effective regime must be in place. Effectiveness should be judged by the capabilities of the regime to supervise and investigate governmental intrusion, the power it has to bring officials and ministers to account, and the transparency it embodies so the public can be confident it is working properly. There should also be means independently to investigate complaints.
6. **Recognition of necessary secrecy**: The 'secret parts of the state' must be acknowledged as necessary to the functioning and protection of the open society. It cannot be more than minimally transparent, but it must be fully democratically accountable.
7. **Minimal secrecy**: The 'secret parts of the state' must draw and observe clear boundaries between that which must remain secret (such as intelligence sources or the identity of its employees) and all other aspects of its work which should be openly acknowledged. Necessary secrecy, however, must not be a justification for a wider culture of secrecy on security and intelligence matters.
8. **Transparency**: How the law applies to the citizen must be evident if the rule of law is to be upheld. Anything that does not need to be secret should be transparent xiv A Democratic Licence to Operate to the public; not just comprehensible to dedicated specialists but clearly stated in ways that any interested citizen understands.
9. **Legislative clarity**: Relevant legislation is not likely to be simple but it must be clearly explained in Codes of Practice that have Parliamentary approval, are kept up-to-date and are accessible to citizens, the private sector, foreign governments and practitioners alike.
10. **Multilateral collaboration**: Government policy on intrusion should be capable of being harmonised with that of like-minded open and democratic governments.

2.1 Directed Surveillance

Surveillance is directed surveillance 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 (whether or not one specifically identified for the purposes of the investigation or operation); 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 this Part to be sought for the carrying out of the surveillance.

Intrusive surveillance is that which takes place on residential premises or on a vehicle, either through the presence of an individual or a surveillance device.

2.2 Covert Human Intelligence Source (CHIS)

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 within paragraph b) or c)
- 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

2.3 Private Information

Private Information is information relating to a person's private or family life. It should be taken generally to include any aspect of a person's private or personal relationship with others, including professional of business relationships.

A person may have a reduced expectation of privacy when in a public place.

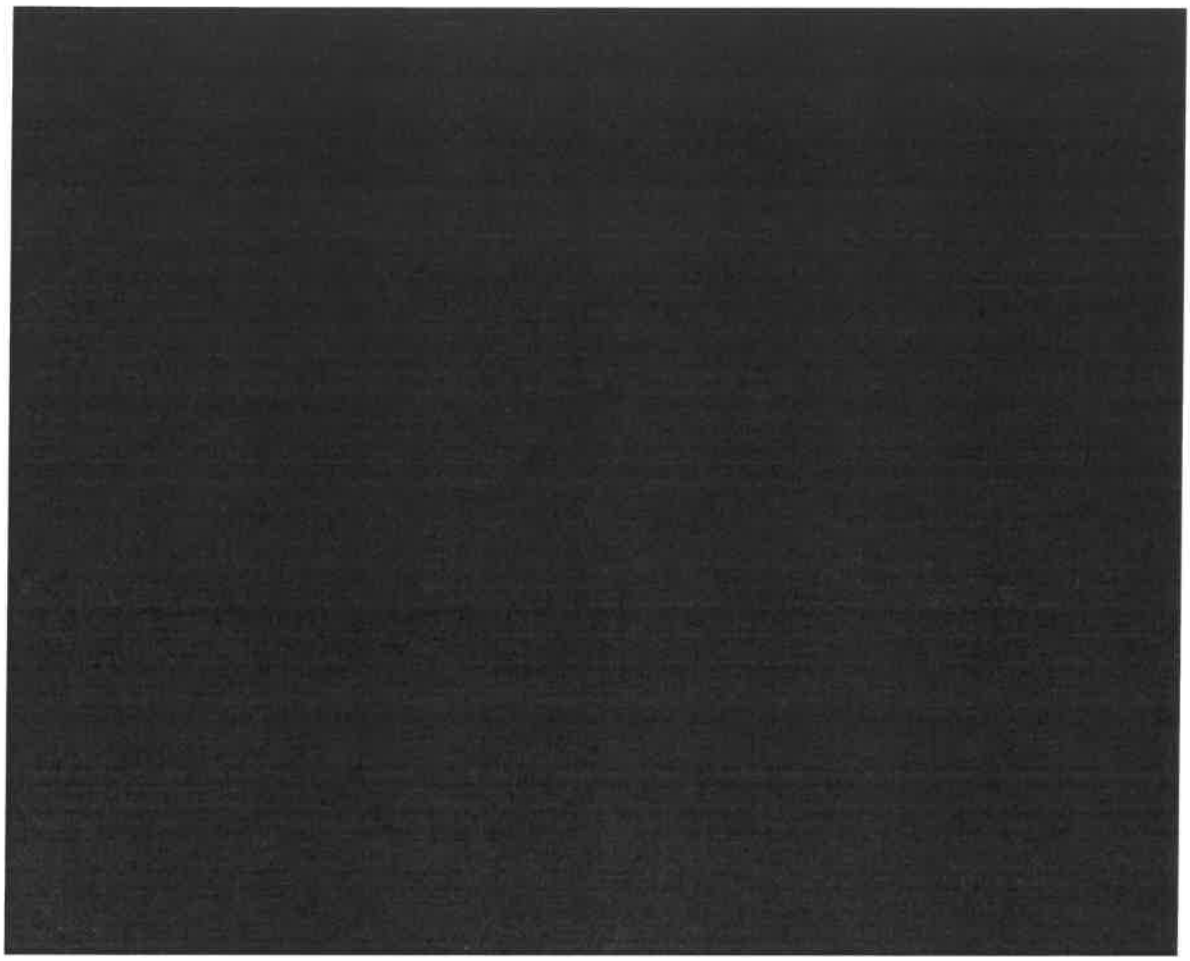
However, covert surveillance of a person's activities in public may still result in the obtaining of private information.

For example, two people holding a conversation on the street or other public place may have a reasonable expectation of privacy over the contents of that conversation.

This proviso is likely to apply to Social Media Sites whether or not access controls such as the 'friends' control in 'Facebook' have been activated.

3. OPERATIONAL RISK CONSIDERATIONS

[redacted]



3.7 Staff carrying out any type of open source investigation/research over the Internet **must be appropriately trained**[2].

4. Evidence

4.1 Processes must be in place to fully record and evidentially capture the content of a webpage that may contain material that is of evidential value. This must be available at a later date for audit or examination.

4.2 Forces should have processes in place that assure the integrity of evidence for its life from capture to court. Evidence should always be corroborated or attributed in some way, but it is important to note that hashing is not sufficient for either purpose. Hashing can be used to demonstrate that two files are identical, making it good for searching for a known file, or checking if something has changed in transit.

[2] Level 1: current ncalt training as per P4, awaiting formal commission of L1 OS training

[redacted]

4.4 Any activity undertaken must be assessed to determine if an authorisation under RIPA is required. In particular a directed surveillance authority (DSA), if in doubt seek advice from your covert authorities' bureau. If a decision is made not to apply for a DSA this together with the rationale should be appropriately recorded.

[redacted]

4.7 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 still has a reasonable expectation of privacy if access controls are applied. Officers should always consider the requirements of RIPA and decisions must be on a case by case basis. In some cases data may be deemed private communication still in transmission (instant messages for example)

4.8 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)

4.9 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 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 who, consent is being sought must be clear what is and is not to be done.

[redacted]

[3] Social Networking Sites

[redacted]

6 Levels of Internet Investigation/Research

6.1 These 5 levels have been approved nationally to define the levels of activity for Open Source Intelligence/research (OSIR) [redacted]

6.2 **The first three levels are open source investigation/research;** [redacted]

6.3 The criteria detailed in the following standards should be seen as minimum to carry out operational activity on the Internet. Departments should assess their operational requirements individually and set operational criteria accordingly as long as it does not fall below the minimum standard.

Level 1 Overt Open Source Investigation/Research (First Responder)

- Conduct research across publicly accessible search areas of the Internet such as map viewing, street views, local authority sites, auction sites or any publicly available website which has no requirement to register details to gain access. As the investigation/research activity is considered overt there is no requirement for any RIPA or Police Act Authority.
- No level of authority but must adhere to force policy regarding use of Computers
- Staff conducting this activity will have received level 1 training[4]

[redacted]

Level 2 Core Open Source Investigation/Research (Intelligence and Investigation)

- Intelligence, investigation/research across publicly accessible search areas of the internet [redacted]
- Level of Authority - none as standard but active consideration should be given to a Directed Surveillance Authority under RIPA on a case-by-case basis.
- [redacted]
- Staff conducting more in-depth open source investigation or research to assist their Investigations.

[redacted]

[4] Ncalt packages ref on P4 pending L1 OS package

[redacted]

- Must be able to evidentially capture and store
- Product recovered must be evaluated and submitted into Force/Agency intelligence management system in most cases using a 5x5x5.

Level 3 Advanced Open Source Investigation/Research (Open Source Unit)

- **Advanced Open Source Intelligence investigation/research**
- Level of authority - on a case-by-case basis with a higher likelihood of a requirement for an authorisation under RIPA
- Training required – recognised advanced open source training to include relevant legislation and case law

[redacted]

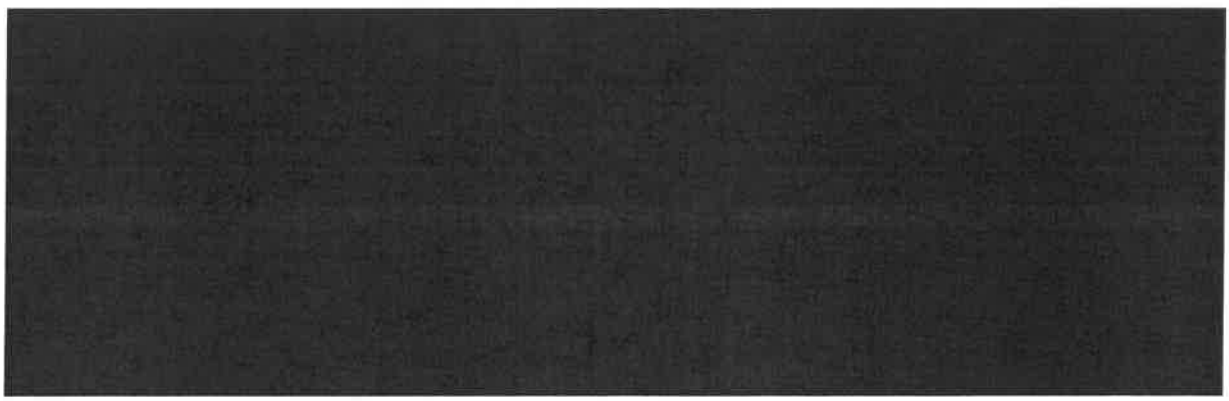
- Must be able to evidentially capture and store

[redacted]

- Product recovered must be evaluated and submitted into Force/Agency intelligence management system in most cases using a 5x5x5.

Level 4 [redacted]

- Must be able to evidentially capture and store



7. Other considerations

[redacted]

7.2 Users should always seek to validate and attribute on-line sources to ensure they are genuine.

[redacted]

8. NCALT and College of Policing Training

Digital Communications - social media, cyber crime and policing (mandatory for all officers, staff, Special Constabulary (MSC) officers and contractors.)

- Cyber Crime and Policing - introduction (mandatory for all federated officers, MSC officers, and staff who work as Researchers and Analysts who have contact with the public, or have reporting and investigative duties.)
- Cyber Crime and Policing - first responder (mandatory for all federated officers, MSC officers, and staff who have reporting and investigative duties.)
- Cyber Crime and Policing - investigations (mandatory for all federated officers, MSC officers, and staff who work with reporting and investigative duties.)