Internet Research and Investigations Protocol

Guidance to enable Scottish local authorities to authorise and control necessary online investigations by their Trading Standards teams

Developed by:

The Society of Chief Officers of Trading Standards in Scotland (SCOTSS)

Endorsed by:

Society of Local Authority Chief Executives and Senior Managers (SOLACE - Scotland)

Society of Local Authority Lawyers & Administrators in Scotland (SOLAR)

Scottish Local Authority Information Security Group (SLAISG)

4 July 2024 – Version 1.0

Table of Contents

1. PURPOSE

1.1 This document provides a framework to enable local authorities to authorise and control necessary online investigations by their Trading Standards teams. It is likely that it can be adapted for use by other local authority investigative teams such as Environmental Health, Planning Enforcement etc. It is endorsed by SOLACE, SOLAR, SLAISG and SCOTSS and its creation follows a recommendation from the COSLA Community Wellbeing Board. The document outlines the activities that are appropriate in relation to accessing information on the internet to conduct research and investigation for a trading standards purpose.

1.2 Scottish local authorities have statutory duties to enforce a wide range of legislation that comes under the remit of their Trading Standards teams. This includes, but is not limited to:

- Scams and other false and misleading activities by businesses
- Protecting consumers from dangerous goods
- Intellectual property, including trade marks and copyright
- Consumer buying rights and contract terms
- The supply of age restricted products such as tobacco, vapes and fireworks
- Fair and accurate weighing, measuring, and pricing of goods for sale.

All these activities take place in both the traditional "real world" of shops and markets and online through e-Commerce websites, online marketplaces, and other platforms such as social media. Every year, the online component grows as a proportion of the total of Trading Standards work. A Trading Standards service cannot be effective – and a local authority cannot fulfil its statutory obligations – without being able to operate successfully online.

1.3 The internet and in particular social media sites can be a rich source of intelligence and on occasion can provide information of significant evidential value. This applies to the full scope of Trading Standards topic areas and to a variety of types of activity, ranging from constructive and positive engagement with legitimate traders over compliance issues through to formal investigations into serious contraventions of Trading Standards laws. Appropriate activities can take place either on standard networked computers or on specialist "standalone" equipment.

1.4 A three-tier model has been developed which identifies the various overt and covert techniques and identifies the level of authority and training etc that is required.

1.5 The primary purpose of this document is to provide the necessary information to ensure that Trading Standards investigators can conduct internet enquiries, at an appropriate level, in a professional manner, without bringing adverse risk to their local authority or having evidence excluded from court, and while respecting individual human rights.

1.6 Some of the activities discussed in this Protocol are subject to the provisions of the Regulation of Investigatory Powers (Scotland) Act 2000 ("RIPSA"). This document does not provide detailed instructions and processes for authorisations and other activities under RIPSA. It is recommended that each local authority has a documented policy for its use of RIPSA to cover such details.

2. INTERNET RESEARCH & INVESTIGATIONS

2.1 Definitions and References

The following definitions and references are used in this document:

"Trading Standards investigator" means any officer that has been authorised by a local authority to use powers to enforce Trading Standards laws and as such includes Managers, Trading Standards Officers, Authorised Officers, Enforcement Officers and others.

"Trader" means anyone selling or supplying goods, services or digital content in the course of a business and subject to Trading Standards laws, including companies, partnerships and sole traders.

"Pseudonym" is an invented fictitious name (a pseudo-identity), used as an alias and in particular to provide credentials for covert purposes.

"Covert profile" means a profile set up on a social network using a pseudonym together with associated email address(s), primarily for the purposes of covert surveillance and covert interactions with profiles under investigation. Covert profiles are developed and maintained in order to keep them relevant and credible through a process known as 'legend building'.

"Overt profile" means a profile set up on a social network using the official credentials of the investigator, primarily for the purposes of overt observations and inspection of business profiles on the same platform, and perhaps to communicate with profiles via platform messaging systems.

"Open source" means information obtained from publicly available sources and not using specialist tools or through invoking law enforcement powers.

"OSINT" stands for Open-Source Intelligence. It refers to the process of collecting and analysing information from publicly available sources to gather intelligence and insights.

"RIPSA" means the Regulation of Investigatory Powers (Scotland) Act 2000

"Directed surveillance" means covert surveillance carried out:

- *for the purposes of a specific investigation or a specific operation;*
- *in such a manner as is likely to result in the obtaining of private information about a person*
- *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 RIPSA to be sought for the carrying out of the surveillance.*

"COVERT_CODE" is a reference to the Scottish Government's Covert Surveillance and Property Interference Code of Practice

"Covert human intelligence source" (CHIS) means a person who establishes or maintains a personal or other relationship with another person for the covert purpose of facilitating anything that:

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

"CHIS_CODE" is a reference to the Scottish Government's Covert human intelligence sources Code of Practice

"Digital evidence" is defined as "information or data, stored or transmitted in binary form that may be relied on as evidence"; source: BS EN ISO/IEC 27037:2016: 'Guidelines for identification, collection, acquisition and preservation of digital evidence'.

"Networked computer" – is a device provided by the investigator's authority and configured to connect only to network infrastructure controlled by that organisation.

"Standalone computer" - is a device not utilising the investigator's internal corporate computer network, but which instead accesses the internet through dedicated internet connections, independent of those mentioned above. For example, a laptop connected to a commercial broadband service on a dedicated telephone line or fibre connection, separate from corporate infrastructure. Further, a standalone device is one that has been sourced specifically for the purpose and which has no software attributed to local authority, any other Law Enforcement Agency or Government body.

2.2 Equipment

2.2.1. Those conducting internet research and investigations to obtain digital evidence should be aware that on every occasion a computer accesses the internet it will leave a footprint. Providers of websites and applications can and will record the IP addresses of persons using their services. In the main part this is not a threat to Law Enforcement conducting overt enquiries as the information, if gathered, is mainly used for commercial purposes etc. Less scrupulous website providers may use this information to identify Law Enforcement Officers who are conducting enquiries e.g., Trading Standards investigators making enquiries on networked computers - a reverse IP lookup would easily identify those making the enquiries. Installing a virtual private network (VPN) could be considered if appropriate.

2.2.2. Accordingly, there is a need for a standalone or covert computer to be available to Trading Standards investigators in order for them to carry out all their functions effectively. Many of the more advanced activities described in section 3 below as "Tier 2" and "Tier 3" should be carried out on such a computer.

2.2.3. However, it should also be noted that a great many more activities can be carried out using a networked corporate computer.

2.2.4. Using a networked computer, investigators carrying out overt research can carry out activities including:

- Screenshots of business webpages for monitoring and market surveillance purposes.
- Overt OSINT searches and capturing publicly available information such as interrogating the Scottish Assessors Association Portal www.saa.gov.uk for details of business operators.
- Screen recording a sample transaction on a trader's website to assess compliance with e-commerce legislation, in particular with the aim of highlighting deficiencies to the business.

2.3 Human Rights

2.3.1 Intelligence gathered from openly available information on the internet or elsewhere is often referred to as OSINT (Open-Source Intelligence). Although this information is referred to as Open Source, all activity intended to gather intelligence for a law enforcement purpose, from whatever source, must be compliant with current legislation, in particular RIPSA, the Human Rights Act 1998 and enforcement powers provided by the Consumer Rights Act 2015 etc. All investigative work by Trading Standards must comply with the European Convention on Human Rights and the Human Rights Act 1998. Of particular relevance to online Trading Standards work is that any interference by officers with the right to privacy must be lawful, necessary and proportionate.

2.3.2 There is a particular requirement for authorities to consider whether activities should be authorised under the Regulation of Investigatory Powers (Scotland) Act 2000 ("RIPSA"). The following descriptions of the three-tier model, and the example scenarios in the APPENDIX, provide some guidance in this regard.

2.3.3 Local authorities should have a RIPSA policy and procedures that enable their Trading Standards teams to carry out all their functions. The requirements of RIPSA are very rigorous and compliance with these ensures that local authorities are protected against risks associated with data management, human rights and general reputational issues.

2.4 Disclosure

2.4.1 All staff conducting internet research and investigations must be aware of their obligations with regard to disclosure. All records of activity and captures made must be stored securely to allow revelation and disclosure at a later date, should this be required.

2.4.2 Further advice and practical guidance can be found within the Crown Office Disclosure manual [1].

[1] https://www.copfs.gov.uk/publications/disclosure-manual/

3. THREE-TIER INTERNET RESEARCH & INVESTIGATIONS MODEL

3.1 Introduction

3.1.1 A three-tier model has been devised to provide structure and uniformity to online research and investigations. The tiers are identified as follows:

- Tier 1 – Overt Internet Research
- Tier 2 – Basic Covert Activities
- Tier 3 – Covert Internet Investigations

3.1.2 All local authorities should operate at least to Tier 2, but ideally to Tier 3 to enable the full range of duties to be exercised effectively.

3.2 TIER 1 – OVERT INTERNET RESEARCH

3.2.1 It is appropriate for all Trading Standards investigators to access the Internet to conduct open-source online searches or other research in relation to any enforcement work.

3.2.2 In relation to routine internet research, this would include the following activities:

- Accessing and using search engines
- Viewing cached versions of web pages in search results
- Visiting trusted websites which are not the subject of investigations
- Conducting research of online news media
- Carrying out a routine test purchase
- Capturing online evidence highlighted by a victim or witness
- Accessing online mapping facilities
- Utilising online data sources such Companies House, Planning Departments etc.
- Reverse image searching
- Webpage source code capture and review

3.2.3 In relation to social media, this would include the following activities, when not logged in to any account:

- Check to see if a person has a social media account
- Establish a Person's or group's Unique Identification Number, e.g. a Facebook UserID
- View public profiles or groups to secure evidence or intelligence
- Request the removal of illegal material e.g., illicit goods

3.2.4 It is also appropriate for all employees to access the internet for the purposes of overt communication. This involves contacting businesses via social media to raise compliance matters while clearly identifying as a Trading Standards investigator. This is done using an upfront social media account created for the purpose by the local authority.

3.2.5 Most Tier 1 activity can take place using a networked local authority computer. Local authorities should give their Trading Standards investigators appropriate levels of access to the internet through the corporate network to allow legitimate work. This should include access to sites that may be

restricted for many other employees of the authority, which will be controlled by local policies and processes.

3.2.6 In exceptional circumstances, some Tier 1 activity may be required to take place on a covert computer due to corporate network restrictions.

3.2.7 It should be noted that the repeated and systematic monitoring, of a person's online activity is likely to be directed surveillance, if it is not clear to the subject that such activity is taking place. This includes, for example, systematically monitoring a personal social media profile or page, even where the profile is open, whether logged in to an account or not. Due to the requirement for RIPSA authorisation, this activity will fall within Tier 2 outlined below.

3.2.8 There will be no activity at Tier 1 which requires authorisation in terms of RIPSA. Investigators must take care when operating under Tier 1 that they do not stray into activities covered by Tier 2 (see below).

3.3 TIER 2 – BASIC COVERT ACTIVITIES

3.3.1 Covert Internet Research is where the activities go beyond Tier 1 and involve surveillance of some kind. Examples are:

- Viewing and monitoring closed social media profiles or pages to secure evidence or intelligence
- Joining and monitoring closed groups
- Conducting systematic surveillance on social media
- Taking simple steps to make a test purchase.

As soon as an investigator is considering these types of activities, they must consider the implications of operating in "Tier 2", for example whether RIPSA applies.

This work does not require significant technical expertise and most of the skills used are those of an investigator and so authorities should not be overly restrictive in their approach to authorising officers to carry out Tier 2 work. However, consideration should be given to the necessary levels of knowledge and experience required before authorising officers to conduct this work and existing enforcement staff should not be automatically authorised.

3.3.2 Many of these activities will require the use of a pseudonym. The creation and use of pseudonyms must be controlled by an appropriate process and documented accordingly. Where information is required from a social media platform that needs a username and password to access the online space (and it is technically unavoidable otherwise) then it is accepted that a covert profile using a pseudonym will be required. It is recommended that a pool of disposable profiles specifically set aside for basic covert investigations is created and managed for these purposes. These simple covert profiles should contain only the minimal information for creation and survival.

3.3.3 Tier 2 research will require a Directed Surveillance Authorisation in terms of RIPSA. Tier 2 does not involve significant and repeated interaction with subjects to the extent that a "relationship" is formed in terms of the concept of Covert Human Intelligence Source (CHIS) in RIPSA.

3.4 TIER 3 - COVERT INTERNET INVESTIGATIONS

3.4.1 Covert Internet Investigation involve sensitive law enforcement tactics that should only be utilised in serious cases. Typically, investigators are deployed on the internet to interact with other users by means of a pseudonym. This may involve "maintaining a relationship" with the subject such that the activity requires authorisation under the Covert Human Intelligence Source (CHIS) provisions of RIPSA. Examples include:

- Repeated messaging where the conversation is not restricted to routine requests for information about purchasing goods or services.
- Communications aimed at uncovering details about the subject's identity
- Communications aimed at uncovering details about the subject's activities, e.g. where they were at a certain time

3.4.2 No RIPSA authority is required to engage online specifically for the sole purpose of arranging a test purchase. If the interaction expands beyond the sole purpose for whatever reason, then an authorisation under RIPSA is required. This would include, for example:

- Where the test purchase is combined with monitoring of a person's online activities (requirement for directed surveillance authority at Tier 2)
- Where the test purchase requires a covert relationship to be established and maintained over a period of time, beyond simply establishing lines of communication with the subject and making a request to purchase goods or services (requirement for directed surveillance, along with CHIS authorisation as appropriate, at Tier 3)

3.4.3 Activities at Tier 3 must include consideration of entrapment under the law of evidence and criminal procedure. Covert Internet Investigators should not, under any circumstances, act as "agent provocateur", i.e. inciting, instigating, persuading, pressurising or cajoling a person into committing an offence that, otherwise, would not have been committed. At all times, covert internet investigators must act in the same manner as an ordinary member of the public would, in the circumstances concerned.

3.4.4 Trading Standards investigators authorised for these activities should have undergone appropriate training or have sufficient previous experience of covert activities to enable effective working. Expertise will generally be at a higher level than for Tier 2 work.

3.4.5 Tier 3 involves covert activities that go beyond standard enforcement work and some consideration must be given to risk and the health and safety of staff. However, given that the work is entirely online, anonymous and generally not involving complex and long-lasting relationships with subjects, it is low risk in the context of CHIS. Local authority RIPSA and Health and Safety policies should take account of these matters and reflect the real level of risk involved.

4. LIST OF ASSOCIATED LEGISLATION/REFERENCE MATERIALS

- Human Rights Act 1998
- European Convention on Human Rights
- Regulation of Investigatory Powers (Scotland) Act 2000
- Computer Misuse Act 1990
- Data Protection Act 2018 / the UK GDPR as defined therein.
- Covert Surveillance and Property Interference Code of Practice (COVERT_CODE)
    - https://www.gov.scot/publications/covert-surveillance-property-interference-code-practice/
    - In particular the section on Online Covert Activity (Paras 3.11 – 3.16)
- Covert human intelligence sources: Code of practice (CHIS_CODE)
    - https://www.gov.scot/publications/covert-human-intelligence-sources-code-practice/
- ACPO/NPCC Good Practice Guide for Digital Evidence
    - https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf
- Council of Europe - Octopus Cybercrime Community
    - https://www.coe.int/en/web/octopus/home

5. Appendix: Example Scenarios

EX.	SCENARIO	ANALYSIS	TIER STATUS
1	An investigator is researching the trading practices of Mark Hall, the operator of an online discount jewellery business with the website: **www.neckless.uk**. The investigator wants to check the website to verify compliance with Trading Standards legislation.	No RIPSA authority is required to look at the website in this scenario.	Tier 1
2	An investigator is researching the trading practices of an archaeological themed package travel business RUIN HOLIDAYS following several complaints. The business has a website: **www.ruinholidays.co.uk** The investigator wants to check the internet site to ascertain compliance with Trading Standards legislation as well as collecting any other information about the business, in particular about who operates it and also who hosts the website.	No RIPSA authority is required to look at the website in this scenario or to conduct online searches (e.g. google) related to the business, including establishing key proprietor information. Establishing the identity and location (including IP address) of the Web hosting company, whose role is to maintain and store the website is also permitted without authorisation.	Tier 1
3	An investigator is conducting enquiries into product safety issues stemming from a new eBay marketplace seller account operated by a company CHEAP TOYS LIMITED. The investigator wants to review the **LinkedIn** profile of a **Mr Rhys QUAY** to establish if (as suspected) this new business is any way linked to him, albeit he is not a named company officer.	LinkedIn has an option to view profiles in private mode and if enabled the target will not know the name of the reviewer. Accordingly, the investigator could review LinkedIn profile information that is available to all users. Simple reconnaissance of a LinkedIn profile is unlikely to interfere with a person's reasonably held expectation of privacy and therefore is not likely to require a directed surveillance authorisation. But where a public authority is systematically collecting and storing information about a particular person or group, a directed surveillance authorisation should be considered.	Tier 1 → 2

EX.	SCENARIO	ANALYSIS	TIER STATUS
4	An officer wishes to conduct online research on Facebook to identify undisclosed business sellers of motor vehicles, with a view to developing intelligence around these subject(s) and making recommendations for operational action.	In order to view some accounts, it may be necessary for the officer conducting this work to be logged in to a Facebook account. It may also be necessary to join certain Facebook buy/sell groups and to access the relevant Facebook marketplace zone. Again, this example highlights a situation where the activity may fall into a **crossover** between Tier 1 and Tier 2 depending on how the research is conducted. Every Facebook user has a Facebook identity number (UserID). Groups have names but they are also identified by a static GroupID number, and similarly each local marketplace has a distinct location_ID. In addition to the entity identification function, Facebook uses these identifiers to form structured searches, many of which can be configured manually in advance by an investigator. For example, a seller's group activity can be determined by invoking a standard search script in the form **facebook.com/groups/GROUPID/user/USERID.** For example, if an officer is looking at posts by Facebook user **1111111** on group **8888888**, the following link will provide that information, separated from the user's other Facebook data: - **https:/ /www.facebook.com /groups/8888888/user/1111111** Similarly, if an officer wishes to examine the overall Facebook Marketplace activity of user 1111111, this pre-built script will display those details: - **https:/ /www.facebook.com /marketplace/profile/1111111** Officers using these focussed searches when conducting initial enquiries may fall into Tier 1 as they avoid much of the collateral information stored within a user's profile, hence arguably no RIPSA authority would be required (see para 3.16 COVERT_CODE). However, when the investigation or research is part of an ongoing piece of work involving repeated viewing of the subject(s), RIPSA authority for directed surveillance should be sought.	Tier 1 → 2

EX.	SCENARIO	ANALYSIS	TIER STATUS
5	An officer wishes to conduct online research on Facebook, to identify prolific sellers of counterfeit goods on Facebook, with a view to developing intelligence around these subject(s) and making recommendation(s) for operational action.	In order to view some accounts, it may be necessary for the officer conducting this work to be logged into a Facebook account. It may also be necessary to join certain Facebook buy/sell groups and to access the relevant Facebook marketplace zone. Given this research is likely part of an ongoing piece of work involving repeated viewing of the subject(s), RIPSA authority for directed surveillance should be sought. Note: If necessary, this research could feasibly be carried out using an overt (or covert) profile on a networked machine, rather than a covert profile on a standalone computer. The reason for this is that research of this nature will not alert the target that their profile was viewed. This is because Facebook does not alert users about who has viewed their profile unless the researcher (perhaps unwittingly or accidently) likes or follows the profile, after which the user will know about that interaction. https://www.facebook.com/help/205685226136386	Tier 2
6	An officer is tasked with making enquiries regarding two pieces of intelligence received that claim that a Jane DOE is selling counterfeit clothing and footwear using social media. Having viewed the target's social media sites, the officer is quickly satisfied that the allegations are credible, and that systematic monitoring is required in order to take the investigation further.	The initial "look" at the target's social media accounts can be carried out at Tier 1. For ongoing and systematic monitoring of these accounts, RIPSA authority for directed surveillance should be sought.	Tier 2

EX.	SCENARIO	ANALYSIS	TIER STATUS
7	An officer wishes to conduct online research on TikTok, to identify sellers of dangerous soother (baby dummy) holders and dummy clips in their region as part of a Scotland-wide sampling and testing initiative.	Although some basic searches can be carried out without being signed into an account e.g. https://www.tiktok.com/search?q=dummy%20clips, in order to view some TikTok accounts, it may be necessary for the officer conducting this work to be logged into a TikTok account. It may also be necessary to FOLLOW certain TikTok profiles. Given this research is likely part of an ongoing piece of work involving repeated viewing of relevant subject(s), RIPSA authority for directed surveillance should be sought.	Tier 2
8	Intelligence is being reviewed by a TS investigation team which indicates that Ms Fay CAKE is selling a large volume of counterfeit clothing on Facebook, publicly through a local Facebook Group entitled 'DONEDEE BARGAINS'. Intelligence suggests the seller is travelling to Turkey monthly to obtain counterfeit garments. In the circumstances, it is reasonably suspected that Ms CAKE is operating in the course of trade or business and acting in breach of Section 92 Trade Marks Act 1994. The case has been referred for an attempted test purchase to be made using a covert account which is aimed at establishing the subject's location and identity.	RIPSA authority is, strictly speaking, not required where activities only involve exercising a power to conduct a test purchase under Para.21 of Sch.5 to the Consumer Rights Act 2015. If however, as part of the investigation, we are routinely monitoring the 'DONEDEE BARGAINS' group in conjunction with Ms Cake's own Facebook page to gather evidence of the volume of goods being sold over a period of time, then RIPSA authority for directed surveillance should be sought. As indicated above, where a test purchase is conducted during routine retail (including e-commerce) interactions, any 'relationship' (if established at all) is likely to be so limited in regard to the requirements of RIPSA that a public authority may conclude that a CHIS authorisation is unnecessary. However, if interactions begin to go beyond narrow ordering instructions and enquiries, a CHIS authorisation should be sought. Ref Para 2.15 CHIS_CODE	Tier 2 → 3

EX.	SCENARIO	ANALYSIS	TIER STATUS
9	Intelligence is being reviewed by a TS investigation team which indicates that local man Mr Nick TYNE is selling disposable vaping products to children via his Instagram profile '**VAPES_4_KIDZ**' using direct messaging and arranging to meet the underage buyers at agreed locations/times near schools in the area. Through intelligence available to date, it is reasonably suspected that TYNE is acting in breach of Section 4A of the Tobacco and Primary Medical Services (Scotland) Act 2010. The case has been referred for a test purchase to be made using a covert Instagram account and young person volunteer.	This case involves two interactions, both of which will required to be authorised under CHIS provisions. The first authorisation will involve the officer acting under a pseudonym adopting a young person's profile, most likely created to appear as if from the local area. A second CHIS authorisation for the juvenile volunteer will require to be authorised by the authority's Chief Executive with the necessary risk assessments completed.	Tier 3

4 July 2024 – Version 1.0