Internet Intelligence & Investigations Guidance

III Overt Profiles

Security classification: OFFICIAL
Disclosable under FOIA 2000: YES
Author: Peter Lloyd, Capability Advisor
Force/organisation: NPCC, Internet Intelligence & Investigations Working Group

Owner	CC Carl Foulkes / III Working Group
Version Number	V 0.5
Date Published	Draft

Compliance Record

Version Control Table

Version	History of Amendments	Approval Date
0.1	First draft	
0.2	Amendments (FAROS Feedback)	
0.3	Minor changes to para 4.8	
04.	Rewording / correction of para 2.3	
0.5	Minor change to paragraph 4.4 (Inclusion of pay as you go and free email) Minor change to 4.8 (removed ‘Share’)	

Table of Contents

1. Purpose

1.1 The purpose of this document is to provide guidance and clarity with regard to the creations and deployment of Internet Intelligence & Investigations (III) Overt Profiles. This guidance should be read in conjunction with the NPCC III Strategy Document and any local policy of guidance. **Local policy and guidance will always take precedence.**

2. Introduction

2.1. The NPCC III Strategy Document sets out a clear Capability Delivery Model which sets out three capability descriptors;

- Core Internet Use
- Internet Investigations, and
- Covert Internet Investigations

2.2. The use of III Overt Profiles sit firmly with the Internet Investigations capability descriptor. Internet Investigations is defined as;

- A structured, methodical, task driven and planned approach to online research, conducted by a suitably trained *(and current)* individual[1]. Activities which fall into this capability descriptor include, but are not limited to;
    - Using overt profiles to log into and access platforms
    - Utilising advanced search techniques to conduct systematic and focused research.
    - Monitoring online activity in relation to pre-planned and spontaneous events
    - Capturing intelligence and or evidence in support of an ongoing investigation

- No covert tactics will be used for Internet Investigations.

2.3 Internet Investigations incorporate a wide array of tactics and capabilities which allow practitioners to add significant value to any enquiry. A small part of this is the research and analysis of Social Media and Social Networking platforms. Although the option to deploy III Overt Profiles is open to those that are suitably trained, there are a number of consideration which will impact on the selection of an appropriate strategy and the use of specific tactics and tradecraft.

2.4 Whilst there are numerous Social Media and Social Networking platforms each with their own configuration and security settings, this document will highlight key points for consideration prior to deploying of an III Overt Profile, along with providing guidance on the creation and management of such profiles. This document will not

[1] The minimum knowledge, skill and competency required for each Capability Descriptor will be outlined in the Skill Matrix – Appendix B

provide a detailed step by step instruction on the creation of profiles for every relevant platform.

2.5 The use of III Overt Profiles is only one tactic available to a trained 'Internet Investigations' practitioner. Prior to commencing any online investigation it is imperative that an investigative strategy is created and decision log maintained. The agreed tactics, use of III Overt Profiles, rationale and risks consider should be recorded accordingly.

3. Internet Intelligence & Investigations Overt Profiles

3.1. Profiles created to conduct 'Internet Investigations' must clearly indicate that they are being utilised for a policing purpose. Such profiles will be referred to as **III Overt Profiles**. The definition of an III Overt Profile is provided below;

> **III Overt Profile –** A profile designed and created to clearly indicate it is used for a policing purpose. Such profiles should include a disclaimer to state that it is not a crime or incident reporting tool and is not used for public or community engagement.

3.2 It should be noted that III Overt Profiles and those used for Community Engagement are distinct and different. The creation and use of Community Engagement profiles are not dealt with, or commented upon, by this guidance.

4. Creation of III Overt Profiles

4.1 Local policy and guidance must be followed with regard to the creation, recording and deployment of III Overt Profiles. Below are some key points for consideration when creating an III Profile.

4.2 The crucial aspect of III Overt Profiles is that, if viewed by a member of the public, they can be clearly identified as used by Law Enforcement. There is no requirement, or suggestion, that such profiles should include personally identifiable information relating to the investigator using it.

4.3 **Email Addresses / Telephone Numbers** – Most profiles require either an email address or a telephone number during the creation process, to verify a profile. Although, local policy permitting, an official email address can used to create a profile, there is no requirement for this. A pay as you go SIM or an email address, created using a free email service, such as Gmail, can be used. No personal email addresses or telephone numbers should be utilised in creating III Overt Profile.

4.4 **Profile Pictures & Vanity Names** - III Overt profiles may include a relevant crest or logo as a profile picture. The 'vanity name' should clearly indicate its use by Law Enforcement.

4.5 **Bio and Descriptions** – Where a platform provides an opportunity to display a Biography or Description this should be utilised to highlight the profiles use by Law Enforcement.

4.6 **Security Settings -** Where possible, III Overt Profiles should be locked down to prevent any person from posting content on the profile, befriending or following the profile, or interacting in any way.

4.7 **Communications** – Where a platform facilitates some form of communication, be it by public post or private message, this facility should be disabled. Where possible, the profile should contain notification that the profile is not to be used for reporting crime. Available methods for crime reporting should be clearly signposted. Where a platforms direct communication capability cannot be effectively disabled practitioners should consider the implications of See EU Directive 2018/1972. See paragraph 5.6 below. III Overt Profiles should not be used for any form of communication.

4.8 **Account maintenance** – On some platforms to maintain a profile, it must engage with other users, pages, groups or become deleted. If this is required, then it can be deemed acceptable to interact with a force profile, page, group that is used to openly communicate with the public. This can take the form of a like however care should be taken to ensure appropriate security settings are applied to avoid the profile becoming liked, followed or befriended. No comments should be made, by an III Overt Profile, on any platform.

5. Risks & Considerations

5.1 The use of III Overt Profiles raises a number of risk and areas which require further consideration. The following risks and issues should be considered prior to creation and deployment of an III Overt Profile.

5.2 **Necessity** – **Can the information you require be obtained without logging into the platform?** For many platforms there are methods of obtaining limited access without the need to log in.

5.3 **Overt or Covert** – **Will the deployment of an overt profile adversely impact on the investigation?** For many investigations, particularly reactive investigations, the use of an III Overt Profile will have no, or little impact.

5.4 **Reputation – Is it appropriate to create an overt profile on the specific platform?** The creation of an overt profile on some platforms may threaten the reputation of the force. In such cases the nature of the platform, and the potential reputational risk to the organisation, may be a rationale for using an III Covert Profile.

5.5 **Platform Capability – Does the platform allow or facilitate the creation of III Overt Profiles?** On some platforms, the creation of III Overt Profiles has become challenging and is actively discouraged by the platform provider. On occasions when an III Overt profile cannot be created, and there remains a requirement to access the platform, this may form part of the rationale for deploying an III Covert Profile.

5.6 **Communications Platforms – Does the platform allow one to one communication?** If the answer is yes and this option cannot be removed through application of security setting then the profile will either need to be de-activated or monitored when not in use. See EU Directive 2018/1972 Section 285.

5.7 **Impact and consequence – What will the impact and potential consequence of activity utilising an III Overt Profile**? Practitioners should always consider the impact of consequence of deploying an III Overt Profile. Whilst members of the public often get reassurance from a police presence, using such a profile to join an otherwise closed group or area can generate varying responses.

- **A general challenge to your activities**. Whilst you actions may be justified and proportionate III Overt Profiles should not be used for Community Engagement.
- **Challenge your capability**. There will always be those that will attempt to challenge the capability of Law Enforcement. Online this can present itself as individuals making inflammatory and threatening comments whilst taking steps to anonymise their identity.
- **Displace activity**. The presence of an III Overt Profile in a private group can result in any activity of interest being displaced. This is a legitimate policing tactic however it can result in the activity be moved to a more challenging area of the internet.
- **Disinformation**. It is well documented that internet is heavily populated with misinformation. The presence of an III Overt Profile will increase the likelihood of disinformation being feed to a practitioner. As always the verification and validation of information gathered online is a key part of the III discipline.

6. Summary

6.1 The creation and deployment of III Overt Profiles is just one of many tactics which fall into the capability descriptor 'Internet Investigations'. This work should only be conducted by suitably trained individuals and in accordance with any local policy and guidance.

6.2 With new platforms regularly being published and established platforms undergoing regular development and improvement, it is impossible to create a step by step guide for each one individually. Security settings and account moderation is constantly changing in the social media domain, so III Overt accounts must be checked periodically to make sure they are still viable and are fit for purpose.

6.3 This document provides some general guidance on the creation of III Overt Profiles, along with relevant considerations for their deployment.