

To: Governance & Audit Committee

From: Mike Hill, Cabinet Member, Community and Regulatory Services
Simon Jones, Corporate Director, Growth, Environment & Transport

Date: 15th November 2022

Subject: Report on use of covert investigative techniques surveillance, covert human intelligence source and telecommunications data requests carried out by KCC between 1 April 2021 – 31 March 2022

Classification: Unrestricted

FOR ASSURANCE

Summary This report outlines work undertaken by KCC Officers on surveillance, the use of covert human intelligence sources (CHIS) and access to telecommunications data governed by the Regulation of Investigatory Powers Act 2000 (RIPA) and Investigatory Powers Act (IPA) during the 2021/22 business year.

Recommendations Members are asked to note for assurance the use of covert investigative techniques during the period and endorse the policy in relation to the use of covert investigative techniques.

1. Background

- 1.1 The document sets out the extent of Kent County Council's use of covert surveillance, covert human intelligence sources and access to telecommunications data. The County Council wishes to be as open and transparent as possible, to keep Members and senior officers informed and to assure the public these powers are used only in a lawful, necessary and proportionate manner.
- 1.2 To achieve transparency and in accordance with the Codes of Practice, an annual report outlining the work carried out is submitted by the Senior Responsible Officer (SRO) to an appropriate Committee. The last report was submitted and approved by the Governance and Audit Committee on 30th November 2021.

2 What this report covers

- 2.1 Covert Surveillance – Surveillance which is intended to be carried out without the person knowing and in such a way that it is likely that private information may be obtained about a person (not necessarily the person under surveillance). Local authorities are only permitted to carry out certain types of covert surveillance and, for example, cannot carry out surveillance within or into private homes or vehicles (or similar “bugging” activity).

- 2.2 Covert Human Intelligence Source (CHIS) – the most common form is an officer developing a relationship with an individual without disclosing that it is being done on behalf of the County Council for the purpose of an investigation. In most cases this would be an officer acting as a potential customer and talking to a trader about the goods / services being offered for sale. Alternatively, a theoretical and rare occurrence would be the use of an ‘informant’ working on behalf of an officer of the Council. In such cases, due to the potential increased risks, KCC has agreed a memorandum of understanding with Kent Police.
- 2.3 Access to communications data – Local authorities can have access to data held by telecommunications providers. Most commonly this will be the details of the person or business who is the registered subscriber to a telephone number or social media account. Local authorities are not able to access the content of communications and so cannot “bug” telephones or read text messages.
- 2.4 In each of the above scenarios an officer is required to obtain authorisation before undertaking the activity. This decision is logged in detail, with the authorising officer considering the lawfulness, necessity and proportionality of the activity proposed and then completing an authorisation document.

After authorisation has been granted (if it is), in relation to surveillance and CHIS, the officer applies for judicial approval and attends a Magistrates’ Court to secure this.

For surveillance and CHIS the approval document is then held on a central file. There is one central file for KCC, held on behalf of the Corporate Director, Growth, Environment and Transport, which is available for inspection by the Investigatory Powers Commissioner (IPC). For telecommunications authorisations KCC uses the services of the National Anti-Fraud Network (NAFN) to manage applications and keep our records. Authorisation for communications data requests is now not carried out by KCC managers but, by law, is undertaken by the Office for Communications Data Authorisations. KCC managers are required only to confirm that officers are seeking authorisation in the course of their duties. Any inspection of this type of approval carried out by IPC is conducted at the offices of NAFN.

3 Covert authorisations carried out between 1 April 2021 – 31 March 2022

Total number of authorisations granted for 2021/22 (figure for 2020/21 in brackets):

Surveillance – 2 (0)

Covert human intelligence source (CHIS) – 1 (0)

Access to telecommunications data – 2 (4)

4. Purposes for which covert techniques used

The CHIS authorisation was used to permit a Trading Standards Officer to pose as a buyer of counterfeit goods in the course of investigating that crime. This case was concluded by the issuing of a “cease and desist” notice to the seller.

One surveillance authorisation was in relation to an operation focussed on the sale of age restricted goods to children. Of the nine premises visited, five made sales. These businesses have received formal written warnings about their conduct. Their future performance in this area is being monitored.

The other surveillance authorisation was in relation to an investigation into organised criminality linked to the sale of various illicit tobacco products. This investigation is ongoing.

One of the telecommunications data requests was in relation to a cross border investigation into fraud linked to the motor trade. This matter is currently before the courts.

The other telecommunications request was in relation to a cross border investigation into false environmental claims. This matter is currently under consideration by counsel in relation to the appropriateness of instigating legal proceedings.

A matter previously brought to The Committee’s attention related to the use of various covert techniques in relation to the investigation of illegal television streaming. Convictions in that matter have been secured and sentencing is awaited.

5. Reportable errors

These are errors which are required, by law, to be reported to the oversight commissioners for either surveillance or communications data requests. The errors can include those made by KCC or those made by third parties including communications data providers.

One reportable error occurred during this year. The error was that an inexperienced Trading Standards Officer used the camera on her mobile telephone to covertly capture images of a market stallholder selling what were believed to be counterfeit goods. The officer had not sought authorisation for this covert activity.

As soon as this action became known to the officer’s manager it was referred to the Head of Kent Scientific Services in his capacity as covert techniques coordinator. The Investigatory Powers Commissioner’s Office (IPCO) were notified on 23rd March, as required, and an internal investigation was carried out. The findings of that investigation were shared with IPCO who responded on 14th April 2022. Their response is attached to this report as appendix 1.

6. KCC Policy

The statutory codes of practice which cover public authority use of covert investigative techniques require that the elected members of a local authority should review the authority's use of these techniques and set policy at least once per year.

Appendix 2 to this report is KCC's policy.

No changes have been made to this policy since it was last brought to this committee.

7. Recommendations

Members are asked to note for assurance the use of covert investigative techniques during the period and endorse the policy in relation to the use of covert investigative techniques.

Contact Officer

Mark Rolfe

Head of Kent Scientific Services

8 Abbey Wood Road

Kings Hill

West Malling ME19 4YT

Tel: 03000 410336

Email: mark.rolfe@kent.gov.uk