

To: Governance & Audit Committee

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

Date: 3rd October 2023

Subject: Report on use of covert investigative techniques surveillance, covert human intelligence source and telecommunications data requests carried out by KCC between 1 April 2022 – 31 March 2023

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 2022/23 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 15th November 2022.

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 2022 – 31 March 2023

Total number of authorisations granted for 2022/23 (figure for 2021/22 in brackets):

Surveillance – 0 (2)

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

Access to telecommunications data – 4 (2)

4. Purposes for which covert techniques used

One of the telecommunications data requests was in relation to an investigation into the sale of a dangerous hair styler. It transpired that the seller is not based in the U.K.

The second telecommunications request was in relation to an investigation into the sale of counterfeit goods and illegal vapes. This application did not elicit any information of value to the investigation.

The third telecommunications request was in relation to an investigation into fraud linked a vehicle repair business. Parallel enquiries suggested that other, less intrusive means of achieving the desired outcome had become available and this application was, therefore, withdrawn before any data was provided.

The fourth telecommunications request was in relation to an investigation into the sale of illegal vapes. This application did not elicit any information of value to the investigation.

5. Update on cases highlighted in last year's report

A case involving the supply of illicit tobacco was highlighted as being ongoing in last year's report. This related to a wide-ranging operation with partners into an organised crime group (OCG) supplying illicit tobacco at various locations in Kent. Disruption tactics were used in this operation, as opposed to prosecution, meaning that quantities of tobacco were seized and closure orders for certain retail premises were secured by our District and Borough Council partners. The current intelligence picture suggests that this activity has been successful and the OCG is no longer functioning in this area.

Two cases in last year's report, one in relation to a motor trade fraud and one into a fraud linked to environmental claims, were described as being before the courts. These cases are still before the courts. There are significant backlogs of cases in the Crown Courts in Kent which are impacting on the delivery of justice in relation to these prosecutions.

The final case highlighted in last year's report related to illegal television streaming fraud. The report said that convictions had been secured but that sentencing was awaited. Two individuals received prison sentences. Billy Martin from London received 21 months and Darren Bough from Dover 2 years. The trial judge described the defendants as 'a couple of Fagins' and explained that the matters were too serious to avoid custodial sentences. He said that the defendants' actions 'struck at the heart on online commerce'.

6. 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.

There were no reportable errors during the reported period.

7. 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.

8. 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

Interim Head of Community Protection

Tel: 03000 410336

Email: mark.rolfe@kent.gov.uk