

To: Governance & Audit Committee

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

Date: 27th September 2021

Subject: Report on use of covert investigative techniques surveillance, covert human intelligence source and telecommunications data requests carried out by KCC between 1 April 2020 – 31 March 2021

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 2020/21 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 21st January 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 2020 – 31 March 2021

Total number of authorisations granted for 2020/21 (figure for 2019/20 in brackets):

Surveillance – 0 (4)

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

Access to telecommunications data – 4 (7)

4. Purposes for which covert techniques used

The 20/21 business year was characterised by the response to the Coronavirus pandemic. This is significant in terms of use of covert techniques as the greatest users of these techniques in KCC is by our Trading Standards Service and a very significant proportion of that service's resources were diverted into carrying out enforcement duties under the various pieces of emergency legislation brought into force to control disease spread.

The impact of this situation on use of covert techniques is that this emergency legislation did not meet the "serious offending" test which local authorities are required to meet before they can engage in the use of covert techniques and, therefore, the use of such techniques by KCC during that year was considerably reduced. Much of the Coronavirus legislation was required to be enforced until September 2021 and it is likely, therefore, that next year's report will also show some reduction in the use of covert techniques.

Use of these techniques during 20/21 was limited to four occasions of access to communications data. All four related to fair trading and consumer fraud type matters. One was in relation to illicit television streaming, one was in relation to a doorstep fraud involving some £86,000 from one victim and two were in relation to a car mileage fraud investigation.

Coronavirus restrictions on the courts have meant that none of the cases currently in the pipeline have been completed.

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.

No reportable errors have been made in relation to KCC authorisations this year.

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 1 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