To: Governance & Audit Committee

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

Date: 18th September 2019

Subject: Report on use of covert investigative techniques surveillance, covert human intelligence source and telecommunications data requests carried out by KCC between 1 April 2018 – 31 March 2019

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) during the 2018/19 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 25th July 2018.

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. This was on the advice of the then Interception of Communications Commissioner's Office (IoCCO). Any inspection of this type of approval carried out by IPC is conducted at the offices of NAFN.

3 RIPA work carried out between 1 April 2018 – 31 March 2019

Total number of authorisations granted for 2017/18 (figure for 2017/18 in brackets):

Surveillance – 5 (5)

Covert human intelligence source (CHIS) – 1 (2)

Access to telecommunications data – 3 (10)

4. Purposes for which covert techniques used

Sale of counterfeit goods

1 Surveillance authorisation, 1 CHIS authorisation and 1 access to communications data authorisations were granted for the purpose of one investigation into the crime of selling counterfeit goods. This is an ongoing, active and high value investigation

Doorstep frauds

4 access to communications data authorisations were granted for the purpose of investigating crimes associated with fraud conducted at homeowners' doorsteps. The crimes include fraud and money laundering. The cases are still under investigation.

Sales of age restricted goods to children

1 surveillance authorisation was granted for the purpose of investigating allegations of sales of age restricted goods, including alcohol and tobacco, to children. Four investigations resulted from sales during this operation.

Fly tipping

1 surveillance authorisation was granted for the purpose of investigating an allegation of fly tipping. No fly tipping was observed.

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.

Since this matter last came to the committee the policy has been updated. Some updates are administrative to, for example, update job titles within the KCC structure. More fundamentally, however, the policy has been updated to take into account changes to the law introduced by the Investigatory Powers Act 2016 which came into force in 2019. Paragraph 7, below, explains those changes.

To adequately reflect the new position the policy is now titled "Policy in relation to the use of covert investigative techniques" rather than referring only to RIPA.

7. New legislation

As highlighted in last year's report, the Investigatory Powers Act 2016 (IPA) has set up a new regime within which local authorities must access communications data. Such access is no longer controlled by RIPA.

A new Office for Communications Data Authorisations (OCDA) has been created and all local authority requests for such data must be channelled through them. Officers will continue to submit their applications via the National Anti-Fraud Network (NAFN) but officers within KCC will no longer authorise these applications. OCDA is a wholly independent body and, as a result, officers will no longer be required to seek judicial approval for authorisations under IPA, saving both officer and court time.

The definitions within IPA also allow local authority officers to seek, in appropriate circumstances, a wider range of information from a communications service provider, beyond the data which was accessible previously. This is likely to have a positive benefit to investigations into serious criminality. Local authorities may not intercept or "eaves drop on" communications. This has only ever been an option for agencies involved in dealing with the most serious offending and national security matters.

The role of Senior Responsible Officer (SRO) under IPA is different from the SRO role under RIPA. The Corporate Director for Growth, Environment and Transport has occupied that role under RIPA and will continue to do so. Whilst the Corporate Director will retain oversight of KCC's use of IPA, the SRO role is more operational and includes the need for engagement with OCDA and also authorisation of certain use of data. The Head of Kent Scientific Services will undertake this role.

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
Head of Kent Scientific Services
8 Abbey Wood Road
Kings Hill
West Malling ME19 4YT

Tel: 03000 410336
Email: mark.rolfe@kent.gov.uk