To: Governance & Audit Committee

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

Date: 25 July 2018

Subject: RIPA report on surveillance, covert human intelligence source and telecommunications data requests carried out by KCC between 1 April 2017 – 31 March 2018

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 2016/17 business year.

Recommendations Members are asked to note for assurance the use of covert techniques under RIPA during the period and the RIPA policy.

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 19th July 2017.

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 telecommunications data – Local authorities can have limited 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. 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 from a named senior officer before undertaking the activity. This decision is logged in detail, with the senior 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) the officer seeking to use the powers 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 2017 – 31 March 2018

Total number of authorisations granted for 2017/18 (figure for 2016/17 in brackets):

Surveillance – 5 (5)

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

Access to telecommunications data – 10 (7)

4. Purposes for which RIPA techniques used

Sale of counterfeit goods
1 Surveillance authorisation, 1 CHIS authorisation and 2 access to communications data authorisations were granted for the purpose of investigating the crime of selling counterfeit goods. Seizures of over 2400

items of counterfeit goods (valued at approximately £100,000) were made and the investigation is ongoing.

Doorstep frauds
1 access to communications data authorisations were granted for the purpose of investigating crimes associated with fraud conducted at home owners' doorsteps. The crimes include fraud and money laundering. The case is still under investigation.

Illicit tobacco sales
3 surveillance authorisations and 4 access to communications data requests were granted for the purpose of investigating illicit tobacco sales including sales of counterfeit products and products which do not meet safety requirements. As a result of this covert activity, seizures of over 130,000 cigarettes, over 350 packs of hand rolling tobacco and over £25,000 in cash were made. These investigations are ongoing.

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. Based on intelligence four premises were subject to an attempted test purchase and one made a sale of tobacco.

Sales of unsafe diet pills
2 access to communications data requests were granted for the purpose of investigating the sale of diet pills containing Dinitrophenol (DNP), an illegal and highly dangerous chemical. Products were seized and a formal warning issued.

Fly tipping
1 access to communications data request was authorised for the purpose of investigating an allegation of fly tipping. The data did not further the investigation.

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 RIPA Policy

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

Appendix 1 to this report is KCC's RIPA policy which has not altered since last reported.

7. New legislation

Some aspects of the Regulation of Investigatory Powers Act, mainly those linked to communications data, are due to be replaced later this year by parts of the Investigatory Powers Act 2016. As yet no firm implementation date has been set but training has been attended in preparation.

8. Recommendations

Members are asked to note for assurance the use of RIPA techniques during the period and the RIPA policy.

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