To: Governance & Audit Committee

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

Date: 19 July 2017

Subject: RIPA report on surveillance, covert human intelligence source and telecommunications data requests carried out by KCC between 1 April 2016 – 31 March 2017

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 the powers 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 27th April 2016.

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 Office of the Surveillance Commissioners. 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 Interception of Communications Commissioner's Office (IoCCO). Any inspection of this type of approval carried out by IoCCO is conducted at the offices of NAFN.

3 RIPA work carried out between 1 April 2016 – 31 March 2017

Total number of authorisations granted for 2016/17 (figure for 2015/16 in brackets):

Surveillance – 5 (3)

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

Access to telecommunications data – 7 (9)

4. Purposes for which RIPA powers used

Sale of counterfeit goods

3 Surveillance authorisations, 2 CHIS authorisations and 2 access to communications data authorisations were granted for the purpose of investigating the crime of selling counterfeit goods. One case has been concluded by means of a formal warning and destruction of the goods, another is currently before the courts.

Doorstep frauds
4 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. A number of cases are currently before the courts or are still under investigation.

Sales of age restricted good to children
2 surveillance authorisations were granted for the purpose of investigating the crime of selling age restricted goods, including tobacco, alcohol and e-cigarette liquids to children. These offences are specifically defined as "serious offending" to permit the use of RIPA techniques.

Unsafe storage of fireworks
1 access to communications data authorisation was granted to investigate the unsafe and excessive storage of explosives in the form of fireworks. The defendants pleaded guilty in court and were fined a total of £12000 with a further £2600 in costs.

5. Results from previous authorisations

A repeat seller of counterfeit goods was convicted and sentenced to 120 days imprisonment (suspended) and £1000 contribution to prosecution costs.

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.

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

7. Other errors

Two non-reportable errors have occurred during this period.

In the first case a surveillance authorisation was properly granted and approved by the court. The officer conducting the surveillance, however, acted outside of the authorisation due to an error in use of the covert recording equipment, meaning that activity was recorded when the officer believed the equipment was switched off. This was identified by the team manager who stopped the surveillance and destroyed the entire surveillance product recorded. The officer has been re-trained to prevent any recurrence.

In the second case an officer and the authorising manager were unaware of a change to the law which brought the sale of e-cigarette liquids containing nicotine to children within the scope of RIPA. The officer, with the manager's agreement, followed all of the RIPA procedures to prevent or reduce unwarranted intrusion but did not undertake the surveillance activity under the RIPA banner and protections. This would constitute a technical

error which did not impact upon citizens' rights to a private and family life. Both officer and manager are now fully aware of the change to the law and information has been provided to other officers updating them on the legal position with this relatively new offence.

8. 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.

9. Recommendations

Members are asked to note for assurance the use of the powers under RIPA 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