

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

To: Governance & Audit Committee

Date: 24th September 2025

Subject: The use of covert investigative techniques surveillance, covert human intelligence source and telecommunications data requests carried out by KCC between 1 April 2024 – 31 March 2025

Classification: Unrestricted

Summary This report outlines the use by KCC Officers of the covert investigatory techniques of surveillance, covert human intelligence sources (CHIS) and access to communications data governed by the Regulation of Investigatory Powers Act 2000 (RIPA) and Investigatory Powers Act (IPA) during the 2024/25 business year.

Recommendations The Governance and Audit Committee is asked to

- (a) note for assurance the use of covert investigative techniques during the period and:
- (b) endorse the policy in relation to the use of covert investigative techniques.

FOR ASSURANCE

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 12th November 2024. The SRO is Simon Jones, Corporate Director for Growth, Environment and Transport.

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, internet address 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 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 IPCO is conducted at the offices of NAFN.

3 Covert authorisations carried out between 1 April 2024 – 31 March 2025

Total number of authorisations granted for 2024/25 (figure for 2023/24 in brackets):

Surveillance – 2 (0)

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

Access to telecommunications data – 1 (8)

4. Purposes for which covert techniques used

One surveillance authorisation was to facilitate an operation carrying out test purchases of vape devices to children using an underage volunteer. Two sales were made. In one case formal warnings were issued to the two company directors and the individual who made the sale. The shop was subject to a licence review and their alcohol licence was revoked. In the second case written warnings were issued to the seller and owner of the business. The business has since ceased trading.

The second surveillance authorisation and the CHIS authorisation were linked to an investigation into the sale of counterfeit designer goods. That matter is still under investigation.

The telecommunications data request was in relation to the activities of a roofing repair business and allegations of fraudulent activity by them. That matter is still under investigation.

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

Last year's report, highlighted a case involving motor trade mileage fraud. That case has now been successfully prosecuted. Three individuals were convicted of conspiracy to defraud by reducing the recorded mileage of used vehicles, mainly light commercial vehicles, by a total of over two million miles. The convicted men were sentenced to a total of 69 months imprisonment, suspended for two years, and each was ordered to complete 200 hours of unpaid work. The trial judge also awarded £37,759 in compensation to the victims.

That report also referred to an investigation of fraud by a vehicle repair business. That business has now been convicted twice, having failed to cease their offending after the first prosecution. Both convictions are awaiting sentencing at the Crown Court as the powers of sentencing at the Magistrates Court have been exceeded.

Reference in that report to a rogue building business with multiple victims was also made. That matter is scheduled to be heard at the Crown Court in February 2026 unless an earlier date can be found.

A fraud linked to a solar energy company was also mentioned in last year's report. That matter is scheduled for Crown Court trial imminently.

6. Reportable errors

These are errors which are required, by law, to be reported to the Investigatory Powers Commissioners Office (IPCO) 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.

A proactive concern was raised with IPCO relating to surveillance carried out linked to waste crime. The commissioners responded that, in their view, the activity was not covert and therefore that no error had occurred.

There were, therefore, no reportable errors during the reported period.

7. Inspection by the Investigatory Powers Commissioners Office

In March 2025 IPCO carried out a remote inspection of KCC's use of the covert investigatory techniques of surveillance and CHIS. This inspection occurs every three years unless serious concerns are raised in the meantime.

Sir Brian Leveson, The Commissioner, confirmed that he was satisfied that compliance with the relevant law will be maintained and confirmed that the next inspection will be due in 2028.

Sir Brian's inspector stated: "Overall, the application and authorisations are completed to a high standard, with appropriate considerations of the statutory grounds of necessity and proportionality".

Some administrative suggestions for improvement were made which have all been built into our practice.

8. 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.

Following guidance from the oversight commissioners, changes have been made to the policy this year to take into account the potential use of artificial intelligence in the assessment of data revealed as a result of using these techniques.

Some minor updates have been made to the forms used to apply for authority to use these techniques. These changes were solely for the purpose of amending the links to the IPC codes of practice, which have themselves been updated.

9. Recommendations

The Governance and Audit Committee is asked to

- (a) note for assurance the use of covert investigative techniques during the period and:
- (b) endorse the policy in relation to the use of covert investigative techniques.

Report Author: Mark Rolfe	Director: Simon Jones
Job title: Head of Community Protection	Job title: Corporate Director for Growth, Environment & Transport
Telephone number: 03000 410336	Telephone number: 03000 411683
Email address: mark.rolfe@kent.gov.uk	Email address: simon.jones@kent.gov.uk