Agenda Item 9

Leicestershire County Council

CORPORATE GOVERNANCE COMMITTEE – 10 MAY 2019

REGULATION OF INVESTIGATORY POWERS ACT 2000 AND THE INVESTIGATORY POWERS ACT 2016

REPORT OF THE DIRECTOR OF LAW AND GOVERNANCE

Purpose of Report

1. The purpose of this report is to:

   (a) advise the Committee of changes to legislation relating to the acquisition of communications data by local authorities; and

   (b) ask the Committee to consider the Covert Surveillance and the Acquisition of Communications Data Policy Statement (previously referred to as the Regulation of Investigatory Powers Act 2000 (RIPA) and Investigatory Powers Act 2016 (IPA) Policy Statement) which is attached to this report.

Policy Framework and Previous Decisions

2. The Codes of Practice made under RIPA require elected members of a local authority to review the authority's use of RIPA and set the policy at least once a year. They should also consider internal reports on the use of surveillance to ensure that it is being applied consistently with the local authority's policy and that the policy remains fit for purpose. Elected members should not, however, be involved in making decisions on specific authorisations.

3. On 20 February 2015 this Committee agreed to receive an annual report on the use of RIPA. On 25 November 2016 this Committee agreed changes to the Council's RIPA Policy Statement to reflect best practice and recommendations of the Office of Surveillance Commissioners (OSC). The Cabinet subsequently approved the revised Policy Statement at its meeting on 13 December 2016 and this was confirmed in 2017 and 2018 to remain fit for purpose.

4. On 24 October 2018, this Committee received its annual report setting out the Authority's use of RIPA for the period 1 October 2017 to 30 September 2018. It would normally have also carried out its annual review of the Council's RIPA and IPA Policy Statement at this time. However, it agreed to delay that review until such time as the Investigatory Powers Act 2016 had

been fully implemented and its effect on the Council's current Policy Statement and processes made clear.

Background

5. RIPA provides a framework to ensure investigatory techniques are used in a way that is compatible with Article 8 (right to respect for private and family life) of the European Convention on Human Rights (ECHR). RIPA ensures that these techniques are used in a regulated way and it includes safeguards to prevent abuse of such methods. Use of these covert techniques will only be authorised if considered legal, necessary and proportionate.

6. The Trading Standards Service is the primary user of RIPA within the County Council and it mainly undertakes the following three activities:

   i. Directed Surveillance – the pre-panned covert surveillance of individuals, sometimes involving the use of hidden visual and audio equipment.
   ii. Covert Human Intelligence Sources – the use of County Council officers, who act as consumers to purchase goods and services, e.g. in person, by telephone or via the internet.
   iii. Communications data – the acquisition of communications data, for example, subscriber details relating to an internet account, a mobile phone or fixed line numbers, but such data does not include the contents of the communication itself.

7. In September 2017 the Investigatory Powers Commissioner's Office (IPCO) took over responsibility for oversight of investigatory powers from the Interception of Communications Commissioner's Office (IOCCO), the OSC and the Intelligence Services Commissioner (ISComm). IPCO are now responsible for the audit functions of these former bodies and will have oversight of the newly formed Office of Communications Data Authorisations as detailed below.

Legislative Changes

8. The Data Retention and Acquisition Regulations (SI 2018/1123) will introduce changes (expected by the end of May 2019) to the way in which local authorities will in future be able to access communications data. The Regulations amend both the Regulation of Investigatory Powers Act 2000 and the Investigatory Powers Act 2016 (IPA) by creating a new authorisation process for public bodies that seek to obtain communications data for a specific criminal investigation.

9. Currently judicial oversight for applications by local authorities to obtain communications data rests with magistrates' courts. This, however, will now be transferred to a new independent body established by the Government, the Office of Communications Data Authorisations (OCDA), which will consider and authorise all future requests.

10. The legislation also requires authorities to enter into a formal collaboration agreement with the National Anti-Fraud Network (NAFN) an organisation, hosted by Tameside Metropolitan Borough Council which specialises in providing data and intelligence services to enforcement agencies. NAFN will in future act as the single point of contact between any communications service provider and the Council and prepare on the Council's behalf any applications to the OCDA.

11. An application to obtain communications data must first receive senior internal approval by the delegated designated person (currently the Team Leader for Civil Litigation and Prosecution) before it can be submitted to the OCDA for consideration. An application will therefore only be referred to the OCDA if it first meets the Council's own necessity and proportionality test.

12. Local authorities will be permitted to acquire the less intrusive types of communications data, now referred to as '*entity' data* (e.g. the identity of the person to whom services are provided) and '*events' data* (e.g. the date and type of communications, time sent, and duration, frequency of communications). However, it will remain the case that under no circumstances will it be permitted to obtain or intercept the content of any communications.

13. In order to obtain either type of data, in addition to satisfying the necessity/ proportionality test, an authority previously had to show the purpose for the application was for the prevention and detection of a crime. This remains the same for *'entity'* data. However, for *'events'* data, the threshold has been raised and the purpose must now be for the prevention or detection of a *'serious'* crime (e.g. an offence for which an individual could be sentenced to imprisonment for a term of 12 months or more, or offences which involve, as an integral part, the sending of a communication or a breach of a person's privacy).

14. Any application to the OCDA will be guided by the Council's revised Policy Statement attached, current best practice and the Communications Data Code.

Recommendations

15. The Committee is asked to:

(a) Note the changes introduced by the Data Retention and Acquisition Regulations (SI 2018/1123);

(b) Recommend to the Cabinet that the revised Policy Statement on the use of RIPA and IPA powers attached as an appendix to this report be approved.

Background Papers

Report to the Corporate Governance Committee on 20 February 2015 and 25 November 2016 – RIPA 2000 Annual Report

Report to the Cabinet on 13 December 2016 – RIPA – Annual Report

Report to Corporate Governance Committee on 24 October 2018 – RIPA 2000 – Annual Report

Circulation under the Local Issues Alert Procedure

None.

Equality and Human Rights Implications

None arising from this report.

Officers to Contact

Lauren Haslam
Director of Law and Governance
Tel: 0116 305 6240
Email: lauren.haslam@leics.gov.uk

Gary Connors
Head of Regulatory Services
Tel: 0116 305 6536
Email: gary.connors@leics.gov.uk

Appendices

Appendix - Covert Surveillance and the Acquisition of Communications Data Policy Statement