Policy on the Acquisition and Disclosure of Communications Data

Version Control

Version Number	Date	Review Date	Author	Reason for new version
01	Jan. 2014		Victoria Simpson	3 year review

Last Updated : February 2014

Victoria Simpson, Lawyer to the Council and Monitoring Officer
victoria.simpson@eastbourne.gov.uk

Introduction

1. Local authorities are empowered to acquire and use communications data in certain circumstances by the Regulation of Investigatory Powers Act ('RIPA') and related legislation. This provides a regulatory framework for certain types of surveillance and data acquisition carried out by local authorities to gather evidence of illegal activity. The Council is aware of the human rights concerns which require it to exercise its powers only in accordance with the law, in situations where doing so is a necessary and proportionate response of last resort.

2. This authority has adopted a policy in relation to covert surveillance (both conducted pursuant to RIPA and outside it) which is available here: http://www.eastbourne.gov.uk/about-the-council/surveillance-and-ripa/.

3. The Council has adopted a policy of not normally conducting covert surveillance but of doing so only as a last resort, where all other investigative options have been deemed insufficient. While each situation will be considered on its own merits and all relevant factors will be taken into account, covert surveillance will be considered only where deemed to be a proportionate response of last resort. A similarly rigourous approach is applied to communications data acquisition under RIPA.

4. What is Communications Data, and what powers do local authorities have in relation to it?

5. Communication data is information about a communication. It can show when a communication happened, where it came from and where it was going. It does not however include the content of a communication, and has therefore been described as the 'who, what and where' but not the 'what', or substance, of the communication.

6. Chapter 2 of Part 1 of RIPA allows local authorities to access communications data about an individual from any Communications Service Provider (CSP), such as a telephone or mobile phone service provider.

7. A new section 23A was added to RIPA by the Protection of Freedoms Act 2012. Just as with directed surveillance or use of a informant, or CHIS, an authorisation or notice to obtain communications data from a CSP shall not take effect until a Magistrate has made an order approving it. The magistrate must be satisfied that:

   a) There were reasonable grounds for the Designated Person (the person authorising the obtaining of the data) within the local authority to believe that obtaining communications data was necessary and proportionate and that there remain reasonable grounds for believing so.

   b) The Designated Person was of the correct seniority within the local authority in accordance the Regulation of Investigatory Powers (Communications Data) Order 2010 (SI 2010/480) i.e. Director, Head of Service, Service Manager or equivalent.

   c) The granting or renewal of the application was only for the prescribed type of communications data to be acquired for the prescribed purpose as set out in the above Order (i.e. subscriber and service use data (e.g. mobile phone subscriber information and itemized call records) to be acquired only for the purpose of preventing or detecting crime or preventing disorder).

8. Policy and Procedure

9. All activity invoking the powers conferred on this authority under RIPA are undertaken in accordance with this document and with regard to up to date and relevant law, including the following:
   - Human Rights Act 1998
   - Regulation of Investigatory Powers Act 2000
   - Protection of Freedoms Act 2012
   - Data Protection Act 1998

10. The Council in addition has regard to relevant official guidance and Codes of Practice, particularly those issued by the Home Office, the Interception of Communication Commissioner (ICCO), the Office of the Surveillance Commissioners (OSC), the Security Camera Commissioner and the Information Commissioner. Officers of the Council use the most up to date forms issued by the Home Office, which are available on their website.

11. Council officers also have recourse to other guidance and resources which have been approved by the Senior Responsible Officer in consultation with the Lawyer to the Council. Enforcement officers are required to contact the Lawyer to the Council or the Senior Responsible Officer for RIPA with any questions or requests for guidance on this topic.

12. This authority subscribes to the National Anti Fraud Network and therefore benefits from recourse to appropriately trained experts who function as this authority's Single Point of Contact insofar as Communications Data is concerned. Subscription to NAFN does not however obviate the need for expertise on this area within this organisation. The Designated Person role is carried out by the Monitoring Officer and Deputy Monitoring Officer at this authority, while the Senior Responsible Officer is the Deputy Chief Executive.

13. The following guiding principles shall form the basis of any covert surveillance activity undertaken by the Council:

- Interception of Communications Dtaa occurs only where it is deemed absolutely necessary to achieve the desired aims. It is undertaken only where it is proportionate to do so and in a manner that it is proportionate.
- Adequate regard is had to individuals' rights and freedoms, and attention is given to the possibility of collateral intrusion.
- All authorisations are granted by appropriately trained and designated Designated Persons ('DPs'), after obtaining judicial approval in accordance with the requirements of the law.

Training and Review

14. All Council officers involved in enforcement are appropriately trained to ensure that they understand their legal obligations and the framework in which their decisions are made.

15. This policy shall be reviewed annually by the Senior Responsible Officer, in consultation with the Lawyer to the Council, in the light of the latest legal developments and changes to official guidance and codes of practice.

16. The operation of this policy shall be overseen by the Council's Audit and Governance Committee, which shall receive regular Reports on this policy and its implementation.

Conclusion

17. While the effective enforcement of criminal and regulatory legislation is vital, the Council only invokes its powers under RIPA as a last resort, where stringent criteria have been met.

18. Adherence to this policy will ensure that where situations arise wherein the Council does elect to invoke the protection afforded by RIPA, it will do so proportionately and in such a way as to involve minimal intrusion into others' lives. This will ensure that any legal challenge to the Council is avoided.

19. Any questions relating to this policy, and any queries regarding the procedure, forms, guidance materials and/or law to be deployed in following it, should be addressed to the officers named below:

Julian Osgathorpe, Deputy Chief Executive

Victoria Simpson, Lawyer to the Council and Monitoring Officer