



To: Leader: Cllr Ian Nimmo-Smith  
Report by: Head of Legal Services  
Relevant scrutiny Strategy & Resources Scrutiny 1/9/2008  
committee: Committee  
Wards affected: None directly

## **REGULATION OF INVESTIGATORY POWERS ACT 2000 Not a Key Decision**

### **1. Executive summary**

- 1.1 This report outlines the powers available to the Council under the Regulation of Investigatory Powers Act 2000 (commonly known, and hereafter referred to, as “RIPA”). It explains the controls in place on the use of the powers and it contains information about the way the powers have been used in practice.
- 1.2 The report is prompted by recent public concern about the use of RIPA powers by local authorities and by a letter sent to all Council leaders in June by Sir Simon Milton, the outgoing Chairman of the Local Government Association. Sir Simon Milton’s letter is appended to this report.

### **2. Recommendations**

The Executive Councillor is recommended:

1. To consider and comment upon the report;
2. To identify any further steps that may be taken to consider or monitor use of the powers discussed in the report.

### **3. Background**

- 3.1 RIPA became law on 25 September 2000, the same day that the Human Rights Act, 1998 took effect. Its purpose was to ensure that a variety of investigatory powers or activities were carried out in a manner compatible with the requirements of the Human Rights Act. It is designed to ensure that public bodies respect the privacy of members of the public when carrying out investigations, and that

privacy is only interfered with where the law permits and where there is a clear public interest justification. The legislation was not passed, as is sometimes suggested, to give local authorities and others powers to fight terrorism, although other agencies (the Police and security services for example) may well use them for this purpose, amongst others.

3.2 There are three types of investigatory powers available to local authorities which are regulated by RIPA. These are:

- i) Covert directed surveillance;
- ii) Use of “covert human intelligence sources”; and
- iii) Access to communications data

The Council can only use these powers for the purpose of preventing or detecting crime or of preventing disorder.

3.3 The report explains the nature of these investigatory powers and the controls that apply to them.

#### **4. Covert Directed Surveillance**

4.1 The Act is designed to regulate the use of “covert” surveillance which is “directed”.

4.2 Covert surveillance is surveillance which is carried out in a manner calculated to ensure that the persons subject to the surveillance are unaware that it is or may be taking place. The use of hidden cameras will amount to covert surveillance as would, for example, secretly following someone to observe what they are doing.

4.3 Directed surveillance is covert surveillance undertaken for the purposes of a specific investigation or operation in such a manner as is likely to result in the obtaining of private information about a person.

4.4 Covert, directed surveillance cannot be used without compliance with the authorisation procedure described later in this report. However, authorisation is not needed if carried out by way of an immediate response to events or circumstances which, by their very nature, could not have been foreseen. For example, a plain clothes police officer would not require an authorisation to conceal themselves and observe a suspicious person who they come across in the course of a patrol.

4.5 The Council cannot authorise covert, directed surveillance which is “intrusive”. This is surveillance of activities within residential premises

or in private vehicles. It amounts to intrusion into people's homes or vehicles either physically or by means of a surveillance device

- 4.6 In practice, the sort of directed surveillance which the Council has undertaken has mostly involved the use of cameras as part of investigation into antisocial behaviour, criminal damage, harassment or unlawful disposal of waste materials.
- 4.7 Whilst the use of concealed CCTV will, in most cases, be regulated by RIPA, the routine use of the Council's public CCTV system is not, as the cameras are not concealed. Nonetheless, the use of overt CCTV is subject to regulation through the Data Protection Act and a detailed Code of Practice is in place to make sure that privacy is safeguarded and that the system is used properly. The Council's CCTV Manager also produces an annual report on the use of the system. This year's report notes that thirteen Police commendations from the Assistant Chief Constable and Southern Division Commander of Cambridgeshire Constabulary were awarded to CCTV staff in the preceding twelve months. The report also records that the team is the current holder of the "CCTV Team of the Year Award", selected at the CCTV User Groups Conference.

## **5. Covert Human Intelligence Sources**

- 5.1 A covert human intelligence source is someone who establishes or maintains a relationship with a person for the purpose of covertly obtaining or disclosing information. In practice, this is likely to cover the use of an informer or Council officer to strike up a relationship with someone as part of an investigation to obtain information "under cover".
- 5.2 Someone who volunteers information to the Council, either as a complainant (for instance, about anti-social behaviour or a breach of planning regulations) or out of civic duty, is unlikely to be a covert human intelligence source. If someone is keeping a record, say, of neighbour nuisance, this will not amount by itself to use of a covert human intelligence source. However, if we are relying on, say, a neighbour to ask questions with a view to gathering evidence, then this may amount to use of a covert human intelligence source.
- 5.3 Use of a covert human intelligence source is subject to the same authorisation regime as the undertaking of covert directed surveillance. However, to date, the Council has not used covert human intelligence sources to undertake investigations.

## **6. Access to Communications Data**

6.1 The Council has power to obtain access to certain types of communications data. These include:

- Traffic data;
- Service use information; and
- Subscriber information.

It is very important to understand that the Council has no powers to gain access to the content of communications under RIPA.

6.2 Examples of the three categories of communications data are set out in Appendix 2 to this report.

6.3 The City Council has never used its powers to obtain access to communications data. It has however considered using the powers in order to detect those responsible for fly tipping of waste in circumstances where discarded mobile phone top-up vouchers may have identified the person responsible for unlawfully tipping the waste.

## **7. Controls**

7.1 This section of the report describes the controls in place to regulate the use of covert directed surveillance. These are similar to the controls applicable to the use of covert human intelligence sources. The controls applicable to communications data are more stringent in that all requests have to be directed through a trained “single point of contact” (currently the Head of Legal Services).

7.2 There is a detailed procedure guide setting out how the Council approaches use of surveillance powers and offering guidance to officers.

7.3 Surveillance powers cannot be used without the approval of an “authorising officer”. Currently only four officers within the City Council may authorise the use of these powers. These are:

- The Director of Community Services;
- The Head of City Homes;
- The Head of Environmental Services; and
- The Head of Legal Services.

All have received training in their role as authorising officers. It is our policy only to appoint named officers at Head of Service or Director level who have first received training.

The following officers have recently received training as authorising officers, in view of the occasional use of these powers made by City Services:

- Director of City Services
- Head of Parking Services and
- Head of Waste and Fleet

The Chief Executive will consider whether they should be given “authorising officer” powers.

7.4 Before surveillance is authorised, an officer must first complete an application form for consideration by an authorising officer. This should set out:

- the reasons why the authorisation is necessary in the particular case and the grounds which make the surveillance permissible – in the Council’s case the only ground is for the purpose of preventing or detecting crime or disorder;
- the reasons why the surveillance is considered proportionate to what it seeks to achieve;
- the nature of the surveillance;
- the identities, where known, of those to be the subject of the surveillance;
- an explanation of the information which it is desired to obtain as a result of the surveillance;
- the details of any potential collateral intrusion and why the intrusion is justified;
- the details of any confidential information that is likely to be obtained as a consequence of the surveillance.
- the level of authority required (or recommended where that is different) for the surveillance; and

- a subsequent record of whether authority was given or refused, by whom and the time and date.

7.5 The authorising officer must then give very careful consideration to the application and decide whether or not it should be approved. The authorising officer needs to take careful account of all the considerations identified above and determine whether the proposed surveillance is appropriate, for a lawful purpose and proportionate. Approval should not be given to tackle relatively trivial matters and, the greater the intrusion into a person's private life, the stronger the justification needs to be. As mentioned earlier, the Council cannot authorise "intrusive" surveillance. If the use of directed surveillance is challenged, it will be for the authorising officer to defend its use – this is not a "rubber-stamping" exercise.

7.6 An approval given to directed surveillance cannot last for longer than three months and dates should be set within that period for review of use of the powers. If they are no longer necessary, or if it becomes apparent that their use is no longer proportionate, the authorising officer should cancel the authorisation.

7.7 The use of directed surveillance beyond the three month period can only take place if the authorising officer agrees, following consideration of a renewal application. Applications to renew an authorisation should include the following information:

- whether this is the first renewal or every occasion on which the authorisation has been renewed previously;
- any significant changes to the information given in the original application for authorisation;
- the reasons why it is necessary to continue with the directed surveillance;
- the content and value to the investigation or operation of the information so far obtained by the surveillance;
- the results of regular reviews of the investigation or operation.

7.8 The Head of Legal Services is sent copies of completed forms and he keeps a central record and takes an overview of authorisations.

## 8. Use of RIPA powers

- 8.1 The City Council is an occasional user of directed surveillance. Typically this involves the use of covert CCTV to identify the perpetrators and/or to gather evidence in cases of serious anti-social behaviour, criminal damage, harassment and serious cases of illegal disposal of waste (fly-tipping). A summary of the use of these powers since January 2007 forms Appendix 3.
- 8.2 Officers are very mindful of the need for considerable care in the use of these powers. The internal Procedure Guide includes the following Statement of Intent:

“Cambridge City Council attaches a high value to the privacy of citizens. It will adhere to the letter and to the spirit of the Act and will comply with this Code.”

However, serious anti-social behaviour, criminal damage, harassment etc can cause considerable distress and misery to those on the receiving end and the victims, quite rightly, look to the Council for some protection. On occasions, the balance will fall on the side of use of these powers even at the expense of some invasion of privacy. Sir Simon Milton’s letter (Appendix 1) clearly recognises this.

- 8.3 The letter goes on to say that “save in the most unusual and extreme of circumstances, it is inappropriate to use these powers for trivial matters”. It then gives the examples of littering and dog fouling as matters falling outside the test of “necessary and proportionate”. The City Council has not used these powers in relation to dog fouling or littering.
- 8.4 There was some recent press coverage of use of the City’s CCTV system to record the number of people begging in the City Centre. Begging has, at times, been a significant issue within the City Centre and we have worked with the Police to reduce the numbers begging. The use of the “overt” CCTV system does not generally fall within RIPA controls, as it is not covert surveillance – the cameras are visible. When we counted the number of people begging, we were not gathering personal information on them – we were doing no more than counting. We also had staff in the City Centre helping with the count late at night and part of what we were trying to do was ensure staff safety. However, this was a non-routine use of the CCTV system and so, to ensure that it was properly considered, we went through the RIPA authorisation procedure.

8.5 The Leader and the Scrutiny Committee are invited to examine the summary at Appendix 3.

## **9. Implications**

- 9.1 The clear implication of this report is the need to ensure that the powers given by RIPA are used with considerable care and that full account is taken of the need to respect personal privacy. However, there will be occasions when the use of these powers is justified by considerations of community safety.

## **10. Background papers**

These background papers were used in the preparation of this report:

Cambridge City Council's "Procedure guide on the use of covert surveillance and "covert human intelligence sources."

## **11. Appendices**

1. Letter of 23 June 2008 from Sir Simon Milton to all Council leaders;
2. Examples of Communications Data
3. Use of RIPA powers by Cambridge City Council since January 2007

## **12. Inspection of papers**

To inspect the background papers or if you have a query on the report please contact:

Author's Name: Simon Pugh, Head of Legal Services  
Author's Phone Number: 01223 - 457401  
Author's Email: [simon.pugh@cambridge.gov.uk](mailto:simon.pugh@cambridge.gov.uk)

## **Appendix 1.**

All Council Leaders

23 June 2008

Dear colleague

As you know, the use by councils of surveillance powers under the Regulation of Investigatory Powers Act (RIPA) has attracted a substantial amount of publicity recently. Most of this has been negative and also often grossly inaccurate; but the news stories have also stimulated public debate and comment concentrating on the line that councils are misusing their powers. The overall effect in terms of the reputation of local government has regrettably been quite damaging.

Parliament clearly intended that councils should use the new powers, and generally they are being used to respond to residents' complaints about fly tippers, rogue traders and those defrauding the council tax or housing benefit system. Time and again, these are the just the type of crimes that residents tell us that they want to see tackled. Without these powers, councils would not be able to provide the level of reassurance and protection local people demand and deserve.

The Act also requires that the powers should only be used when "necessary and proportionate to prevent or detect a criminal offence" and you will all know of the examples where councils have been criticised for using the powers in relation to issues that can be portrayed as trivial or not considered a crime by the public.

My purpose in writing is to ask that you satisfy yourself that the use of these powers is only being authorised after the most careful consideration at the appropriate senior political and managerial level. It would also be helpful if you could review existing permissions to ensure that their continuance meets the "necessary and proportionate" test. Perhaps you might consider reviewing these powers annually by an appropriate scrutiny committee or panel of your council which could invite evidence from the public. Whilst it is a matter for each council to determine for its area, our advice is that, save in the most unusual and extreme of circumstances, it is inappropriate to use these powers for trivial matters.

The leaders of the four political groups at the LGA and I have discussed this issue, in conjunction with the Local Authorities Co-ordinators of Regulatory Services (LACORS), and, specifically, we do not consider dog fouling or

littering as matters which fall within the test of "necessary and proportionate".

The LGA and LACORS are working with the Government, police chiefs and the Chief Surveillance Commissioners to clarify some of the details of the legislation and make sure it is clear when and how surveillance should be used. By their nature, surveillance powers are never to be used lightly but it is important that councils don't lose the power to use them when appropriate. It is not right that councils are being tarred with accusations of using 'anti-terror' powers to investigate local crime when they are doing nothing of the sort. Equally it is important that they use these powers carefully and appropriately and we will be working with you to help enable that.

I hope you will be able to help in the manner I have suggested. Obviously in writing to you I am doing so with the support of all four group leaders here; we would be pleased to hear from you if you have any comments following your review or further suggestions on how as a sector we might ensure that councils' use of these new powers has general public support.

Yours sincerely,

Sir Simon Milton  
Chairman of the Local Government Association

## Appendix 2: Examples of Communications Data.

Communications data falls into one of three categories: traffic data, service use information and subscriber information.

Examples of **traffic data** include

- information tracing the origin or destination of a communication that is, or has been, in transmission (including incoming call records);
- information identifying the location of equipment when a communication is, has been or may be made or received (such as the location of a mobile phone);
- information identifying the sender or recipient (including copy recipients) of a communication from data comprised in or attached to the communication;
- routing information identifying equipment through which a communication is or has been transmitted (for example, dynamic IP address allocation, file transfer logs and e-mail headers – to the extent that content of a communication, such as the subject line of an e-mail, is not disclosed);
- web browsing information to the extent that only a host machine, server, domain name or IP address is disclosed;
- anything, such as addresses or markings, written on the outside of a postal item (such as a letter, packet or parcel) that is in transmission and which shows the item's postal routing;
- record of correspondence checks comprising details of traffic data from postal items in transmission to a specific address, and online tracking of communications (including postal items and parcels).

Examples of **service use** information include:

- itemised telephone call records (numbers called);
- itemised records of connections to internet services;
- itemised timing and duration of service usage (calls and/or connections);
- information about amounts of data downloaded and/or uploaded;

- information about the use made of services which the user is allocated or has subscribed to (or may have subscribed to) including conference calling, call messaging, call waiting and call barring telecommunications services;
- information about the use of forwarding/redirection services;
- information about selection of preferential numbers or discount calls;
- records of postal items, such as records of registered post, recorded or special delivery postal items, records of parcel consignment, delivery and collection.

#### 6.4 Examples of **subscriber information** include:

- ‘subscriber checks’ (also known as ‘reverse look ups’) such as “who is the subscriber of phone number 0 2 3 5 6789?”, “who is the account holder of e-mail account example@example.co.uk?” or “who is entitled to post to web space *www.example.co.uk?*”;
- information about the subscriber to a PO Box number or a Postage Paid Impression used on bulk mailings;
- information about the provision to a subscriber or account holder of forwarding/redirection services, including delivery and forwarding addresses;
- subscribers or account holders’ account information, including names and addresses for installation, and billing including payment method(s), details of payments;
- information about the connection, disconnection and reconnection of services to which the subscriber or account holder is allocated or has subscribed to (or may have subscribed to) including conference calling, call messaging, call waiting and call barring telecommunications services;
- information about apparatus used by, or made available to, the subscriber or account holder, including the manufacturer, model, serial numbers and apparatus codes;
- information provided by a subscriber or account holder to a CSP, such as demographic information or sign-up data (to the extent that information, such as a password, giving access to the content of any stored communications is **not** disclosed save where the requirement for such information is necessary in the interests of national security).

## Appendix 3: Use of RIPA powers by Cambridge City Council since January 2007

The month in which the investigatory powers were utilised	The nature of the investigatory powers utilised	The reason why the investigatory powers were utilised
January 2007	Covert CCTV	Detection of criminal damage and anti-social behaviour. Allegations of serious criminal damage; for example, slashed car tyres, eggs thrown at windows, air rifle pellets fired at windows and cars.
February 2007	Use of City Centre CCTV (not covert)	Count of numbers begging in the City Centre.
March 2007	Covert CCTV	Detection of criminal damage and anti-social behaviour. Anti-social behaviour by a group of young people swearing at members of the public and pushing them off bicycles. Also issues of street robbery and assault.
	Covert CCTV	Detection of criminal damage and anti-social behaviour. Eggs, stones and concrete thrown at residential premises. Five incidents over a period of ten days, resulting in a front window being smashed. Also issues of graffiti.
April 2007	Covert CCTV	Detection of anti-social behaviour. Loud music, assaults, harassing neighbours for money.
May 2007	Covert CCTV	Detection of unlawful fly-tipping. CCTV was used in an attempt to identify those responsible for fly-tipping in a location identified as a fly-tipping "hot spot".
June 2007	Covert CCTV	Detection of unlawful fly-tipping. CCTV was used in an attempt to identify those responsible for fly-tipping in a location identified as a fly-tipping "hot spot". Police interest in the nature of the materials being tipped and this has led to serious criminal proceedings.
July 2007	Covert CCTV	Detection of criminal damage and anti-social behaviour. Criminal damage to school premises. Windows repeatedly smashed over a period. Concern for safety of pupils.
August 2007	Covert CCTV	Detection of unlawful fly-tipping. This related to the repeated deposit in a highway drain of a liquid substance that gave off an offensive smell and had involved the need for the Fire Brigade to visit on several occasions to wash the substance away. Use of CCTV led to the identifier of the perpetrator, who has been cautioned, and the cessation of the nuisance.
December 2007	Covert CCTV	Detection of criminal damage and anti-social behaviour. This related to allegations concerning continuous and repeated ASB by a large group of young people around a residential area.
January 2008	Covert CCTV	Detection of criminal damage and anti-social behaviour associated with residential premises. Use of CCTV followed a successful court application for possession

		and an injunction with a power of arrest. Despite this, witnesses continued to have threats made against them and their property attacked mostly at night. CCTV was particularly needed as the witnesses reported that they were too scared to look out of their windows to identify the perpetrators in case they were seen.
May 2008	Covert CCTV	Covert CCTV authorised to gather evidence to support allegations of racist harassment and criminal damage. The CCTV was to be targeted to cover the rear garden of the alleged victim.
June 2008	Covert CCTV	Harassment/anti-social behaviour. ASB team investigating allegations of drug dealing, prostitution, anti-social behaviour and noise nuisance against an individual, who was making counter-allegations of intimidation and harassment by neighbours. There were suggestions of a "hate campaign" and concerns for safety of the alleged victim and his/her children. CCTV was authorised to cover a communal garden area in a bid to gather evidence.
August 2008	Covert CCTV	Detection of unlawful flytipping. This follows several complaints regarding regular and persistent fly-tipping which is affecting the environmental quality of the area and is attracting other anti-social behaviour. There is a sign in place which reads: "Flytipping Hotspot. This area is monitored by Cambridge City Council CCTV cameras for more information or to report fly tipping in this area call 01223 458573."