Making Northern Ireland Safer For Everyone Through Professional, Progressive Policing

FREEDOM OF INFORMATION REQUEST

Request Number: F 2011 00130

Keyword: Crime

Subject: Cell Phone Monitoring

Request and Answer:

Request

1) Who has access to cell phone co-ordinates once they are switched on (other than the phone companies and any newspaper type hacking their phones)? How many years are they kept for?
2) What legislation is required to have a public servant monitor any person's cell private phone calls?
3) Who authorises cell phones being 'tapped'?
4) Who authorises landlines being 'tapped'?
5) Who can authorise the intrusion of computers?
6) Does it take separate permission for 2/3/4/5
7) Do you have access to audit trails /social user networks/phone trees of any 'suspect'?
8) Who authorises home searches and who conducts such?
9) Do you have the location of everyone residing in your region. If it takes more than their name on an electoral role I would like to know?

Firstly, the Police Service of Northern Ireland (PSNI) would apologise for the short delay in responding.

Answer

Your request asks several questions regarding the abilities the PSNI has to carry out certain monitoring activities. Under the terms of the Freedom of Information Act, we are required to respond to requests for information based on the information held by us at the time the request is received. This means that information that is recorded becomes liable for disclosure. The fact that your request does not clearly specify exactly what recorded information you require, but is more a series of questions requiring a formulated response, would enable us to respond by simply saying there is no information held, albeit that we may have access to various policies, procedures and legislation that answers your questions by virtue of the information contained within them.

Therefore we would provide the following information, available as open public source, to answer your questions.

The legislation that gives authorisation for these activities is covered by the Regulation of Investigatory Powers Act 2000 (RIPA Part I) and The Police Act (Part III). Section 21 (Information reasonably accessible by other means) can therefore be applied to these questions and the applicant

directed to the links below.

http://www.legislation.gov.uk/ukpga/2000/23/contents

http://www.legislation.gov.uk/ukpga/1997/50/part/III

The RIPA act is a regulatory framework around a range of investigatory powers to ensure the powers are used lawfully and in a way that is compatible with the European Convention on Human Rights. It also requires, in particular, those authorizing the use of covert techniques to give proper consideration to whether their use is necessary and proportionate.

RIPA regulates the following areas:

- The interception of communications (for instance, the content of telephone calls, e-mails or postal letters). **RIPA part 1 chapter I.**
- The acquisition and disclosure of communications data (information from communications service providers relating to communications). **RIPA part I chapter II.**
- The carrying out of covert surveillance. **RIPA part II**.
    - in private premises or vehicles ('intrusive surveillance') or
    - in public places but likely to obtain private information about a particular person ('directed surveillance')
- The use of covert human intelligence sources (such as informants or undercover officers). **RIPA part II**.
- Access to electronic data protected by encryption or passwords. **RIPA part III**.

RIPA provides a number of important safeguards:

- It strictly limits the people who can lawfully use covert techniques, the purposes for and conditions in which they can be used and how the material obtained must be handled
- It reserves the more intrusive techniques for intelligence and law enforcement agencies acting against only the most serious crimes, including in the interests of national security
- It provides for the appointment, by the Prime Minister, of independent oversight Commissioners and the establishment of an independent tribunal to hear complaints from individuals who believe the techniques have been used inappropriately (IPT). In the discharge of their functions, the commissioner's and staff carry out a programme of inspection visits, reports and meetings with an annual report is laid before Parliament.

The following bodies oversee the use of RIPA:

Office of Surveillance Commissioner - The OSC's aim is to provide effective and efficient oversight of the conduct of covert surveillance and covert human intelligence sources and investigation of electronic data protected by encryption by public authorities in accordance with Parts II and III of RIPA. Details of the current annual report can be found on the OSC web site.

Interception of Communications Commissioner - The interception of communications commissioner is both in relation to the interception of communications and access to communications data. Police surveillance activity is subject to annual inspection by the IOCCO (Interception of Communications Commissioners Office). These inspections assess each constabulary's compliance with the legislation and a full report is submitted to the Prime Minister and Scottish Ministers.

Question 1 – The location data of mobile telephones is included in the records kept by mobile networks. A limited number of public authorities may, by virtue of Chapter 1 Part 1 RIPA and when necessary and proportionate, acquire the data if included in the interception warrant i.e. related communications data. A broader range of public authorities who have powers within Chapter 2 Part 1 RIPA to acquire communication data (that does not include the content of communications) may, and when necessary and proportionate, require its disclosure. The EU Data Retention Directive requires the retention of location data generated or processed by the mobile networks for a minimum period of 12 months.

Questions 2,3,4,5, and 6 –The answers to these questions are all covered by RIPA Part I, as outlined above.

Question 7
Social networks are no different to other commercial entities the police deal in that they may hold information that may be of use in criminal investigations and it may be appropriate to require the disclosure of information using an order of the court or advise of circumstances which enables the disclosure of the information by means of the Data Protection Act 1998. Such organisations also report crimes they are subjected to as part of their business functions, share their suspicions about the misuse of their services by persons committing crimes (e.g. sexual grooming of children) etc. It is common practice for social networks to their publish terms and conditions as to when it is appropriate to proactively disclose information to the police and when they believe disclosure must be requirement i.e. by the police using a statutory power.

Question 8 –These activities are governed by the Police and Criminal Evidence (PACE) (Northern Ireland) Order 1989 and searches under PACE are authorised by either District Judges or, in certain cases, by police officers (e.g. immediately upon arrest). PACE is only relevant in relation to overt searches. There are a number of pieces of legislation which provide for overt searches of homes, e.g. the Terrorism Act 2000. Part III of the Police Act 1997 allows for trespass on property to be authorised in certain circumstances

The details can be found at:
http://www.legislation.gov.uk/nisi/1989/1341/contents

Question 9 – Police obtain and retain details regarding the names and addresses of persons in a number of situations. This is regulated by legislation, including the Data Protection Act and the Human Rights Act, as well as guidance (Management of Police Information) none of which empower us to actually monitor the current location of every citizen.

If you have any queries regarding your request or the decision please do not hesitate to contact 028 9070 0164. When contacting the Freedom of Information Team, please quote the reference number listed at the beginning of this letter.

If you are dissatisfied in any way with the handling of your request, you have the right to request a review. You should do this as soon as possible, or in any case within two months of the date of issue of this letter. In the event that you require a review to be undertaken, you can do so by writing to the Head of Freedom of Information, PSNI Headquarters, 65 Knock Road, Belfast, BT5 6LE or by emailing foi@psni.pnn.police.uk.

If following an internal review, carried out by an independent decision maker, you were to remain dissatisfied in any way with the handling of the request you may make a complaint, under Section 50 of the Freedom of Information Act, to the Information Commissioner's Office and ask that they investigate whether the PSNI has complied with the terms of the Freedom of Information Act. You can write to the Information Commissioner at Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF. In most circumstances the Information Commissioner will not investigate a complaint unless an internal review procedure has been carried out, however the Commissioner has the option to investigate the matter at his discretion.

Please be advised that PSNI replies under Freedom of Information may be released into the public domain via our website @ www.psni.police.uk

Personal details in respect of your request have, where applicable, been removed to protect confidentiality.