HERTFORDSHIRE CONSTABULARY

Date: 11th February 2011

Our Ref: FOI/018/11

Contact: Alice Duarte

Tel: 01707 638436

Fax: 01707 354669

By email only to: request-57916-b7daad21@whatdotheyknow.com

Dear Mr Gaffney,

Thank you for your request for information on Nodal Analysis. Your specific request has been outlined below.

"Various types of technology are used for uncovering hidden human networks .They are called different things but they employ similar techniques for example:

1. Nodal Analysis (the military version) 'Nodal analysis '.This maps the relationships between different phones and their users. Once this is established their cell phone could be used as means to locate them. Even if the initial conversations don't lead up to anything didn't arouse any suspicion the recording of all conversations and the locations of the cell users allows those with access to sift through all the conversations leading up to something and occasionally to use those records to find out where the persons involved were based. It's perfectly feasible to record all cell phone use in a country not just co-ordinates but the related audio-files. There is what is termed F3EA:
    i. Find the person involved.
    ii. Fix their position in time and space.
    iii. ? him.
    iv. Exploit and Analyse each 'raid' for intelligence gathering purposes for future 'raids'.
2. Link Network Analysis (The civilian version as used by the FBI and the like) 'Link/network analysis'. We examine each subjects social networks ,bank details, audit trails and phone trees….something like the use of nodal analysis with the military ….their own version of 'network centric warfare '.They plug in photos of the subjects ,other clues from available databases ,clues found by agents which builds a 'web' or 'net' of links. Basically they use the subjects own networks against them. Everyone leaves a presence… a ripple…..they're human. If they even are switch on their cell phone they reach out to phone masts to triangulate their positions thus ensuring everyone whether it be myself, a criminal ,a police officer or even a judge or politician can be tracked ...
3. The current generation of cell phone is not far short of an 80's supercomputer .Software on it can be used for a variety of purposes (satellite navigation by means of the worldwide GPS system, location finding by means of triangulating Wi-Fi use ,social networks updates(I have seen various politicians on my Face book profile page showing what a small world it truly is), possibly even the use of Iridium Next technology if they just insert a chip into the next generation cell phones allowing satellite technology to be used ....where reception is poor. My own favourite killer app is the voice stress analyser :see below links)
   http://www.whatdotheyknow.com/request/use_of_modern_lie_detectors#incoming-97148
   http://www.whatdotheyknow.com/request/use_of_modern_lie_detectors_6#incoming-112054
   http://www.whatdotheyknow.com/request/use_of_modern_lie_detectors_5#comment-10612
   http://www.whatdotheyknow.com/request/use_of_modern_lie_detectors_8#incoming-92960
   and Suffolk Constabulary's own..
   http://www.whatdotheyknow.com/request/use_of_modern_lie_detectors_2#outgoing-62467
   (I have copied hundreds if not thousands of solicitors firms (in countries who are ECHR signatories) into that FOI stream just to see if anyone had an interest in the information gleamed.

   The information in this FOI was extracted from a novel I am writing(currently at 14500words) I copied in everyone I e-mail including the solicitor's firms aforementioned with a pdf with the first twenty odd thousand words) My own experience where such technology could be put to use was with a brief encounter with the police of Suffolk Constabulary
   On Friday 14 2011 I was stopped by someone who got out of a car at the corner of Elm Street in Ipswich saying 'I want a word with you'. In Glasgow that would often be precursor to getting mugged. He, I later found he was Detective Constable NO357(I won't disclose his name) .He had stopped me ten minutes after visiting the Crown Court . He, I later found out was directly in front of me in a Crown Court case involving the import and distribution of heroin/ diamporphine given the illegality of said drug in the UK. He accused me of following him though I was on foot and he was in the unmarked police car with a colleague. I made an informal complaint to his line manager (A male Police Inspector) and then later had a brief chat with the court manager at Ipswich Crown Court.

   This problem and many other's like it could have been solved by disclosure of my 'android' phone's co-ordinates and his and his colleague's inevitable cell phone's locations on that day to avoid confusion.

Related FOI Questions

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?

I am able to confirm that your request has been processed under the terms of the Freedom of Information Act 2000 (FOI).You have asked several questions regarding the abilities the force has to carry out certain monitoring activities.

Under the terms of the Freedom of Information Act, the Constabulary is 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). Links to the relevant documentation have been provided below. Therefore Section 21 (Information reasonably accessible by other means) can be applied.

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 which 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 Protections 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 a requirement i.e. by the police using a statutory power.

Question 8
These activities are governed by the Police and Criminal Evidence Act 1984 which is authorised by a Magistrate or in some circumstances by an Inspector in charge of a police station.

Full details can be found at:
http://www.legislation.gov.uk/ukpga/1984/60/contents

Question 9
As outlined above there is no actual 'information held' as it would actually be unlawful to carry out such an activity.

The police keep records of persons and their addresses as part of their administrative function and that function is wide ranging e.g. persons who are or have been in police custody; persons who are wanted on a warrant given by a court; persons who have reported crime, are a victim or are suspected of crime; persons who are witnesses to criminal events; information gathered in the course of an investigation or operation from a multitude of sources which indicate the name and addresses of persons. This is done in compliance with various legislation such as the Data Protection and Human Rights Act, none of which empower us to actually monitor the current location of every citizen.

Yours sincerely,

Alice Duarte

Alice Duarte
Freedom of Information Assistant
Hertfordshire Constabulary provides you the right to request a re-examination of your case under its review procedure. If you decide to request such a review and having followed Hertfordshire Constabulary's full process and you are still dissatisfied, then you have the right to direct your comments to the Information Commissioner who will give it consideration.