



Home Office

BUILDING A SAFE, JUST
AND TOLERANT SOCIETY



Home Office
BUILDING A SAFE, JUST
AND TOLERANT SOCIETY

Public Authorities Use of RIPA

I am a Public Authority What Can I Do?



Home Office
BUILDING A SAFE, JUST
AND TOLERANT SOCIETY

- Comms Data the Golden Thread
- What Information are we entitled to?
- When Can We Spy On People?
- What is the role of the SPOC/SRO?
- Is Your Request Feasible?
- How Quickly Will I Get My Data Back?
- Practical Examples/RIPA Application
- Questions

Comms Data the Golden Thread



Home Office
BUILDING A SAFE, JUST
AND TOLERANT SOCIETY

- The provisions in UK law for relevant public authorities' acquisition of communications data – under Part I Chapter II of the Regulation of Investigatory Powers Act 2000 – make lawful requirements for disclosure of data for the purpose of preventing and detecting crime that are necessary and proportionate in line with respect for Convention Human Rights.
- Communications data is a vital investigative tool that can reveal associations and events by time and location with proven benefits in terms of helping secure successful convictions
- Can show who communicated with whom, when and, for mobile communications, where (but not what was said or written).



Nathan "23" Martin



**Michael "Chunks"
Gregory**



**Robert Firkins &
Lee Firkins**

Comms Data can be the 'golden thread' running through an enquiry providing an indication of associations, times and places. Knowing to whom a phone is registered, what calls were made, when and where they were made, whether answered or unanswered, means we can trace the events leading to a crime and the individuals associated with it.



Home Office
BUILDING A SAFE, JUST
AND TOLERANT SOCIETY

Categories of Data – Where?

- Section 21 (4) (a) – Traffic data
- Available to the Police, Intelligence Agencies & Other Public Authorities that deal with Serious and Organised Crime

- Information identifying any location of a communication (such as mobile phone cell site location data.)

- Internet Routing Information

- Web activity logs are only retained for a short period of time typically between 0-4 days.

- Incoming call data

- All traffic data retained for a period of one year. The data automatically drops the systems on a daily basis and is not generally archived..



Home Office
BUILDING A SAFE, JUST
AND TOLERANT SOCIETY



Categories of Data – Who/When?

- Section 21 (4) (b) – Service Use information
 - Outgoing call records
 - Call record data (switch records) are retained for between 6 – 18mths. The data automatically drops off the systems on a daily basis and is not archived.
 - Copy invoices are held for six years. Copy invoices (bills) are a duplicate of what was sent to the customer. A copy bill may not necessarily itemise every call made as ‘free time calls’ may just appear as summary (number of calls made and the length.)
 - Internet
 - Log on/Log off data, assigned IP addresses and email are typically kept between 0-6mths because of the large volumes of internet traffic it is currently difficult to keep them for longer periods.

Categories of Data- Who?

- Section 21 (4) (c) – Subscriber information
 - Who is the subscriber (owner) of a certain telephone number
 - Historically, in most cases a CSP should be able to locate subscriber information going back 1 or 2 years. Remember that telephone numbers are re-used after a period of hibernation so the same telephone number can be issued more than once.
 - A vast majority of mobile customers are unregistered prepaid accounts. However if a prepaid account is registered, address details are not verified.
 - Payment methods
 - E-top up data
 - Credit card payments/direct debit details

Categories of Data

- Customer contact notes
 - In most cases, customer contact notes are deleted after 12-18 months. This would include any change of address details
- Copy contract/agreement forms
 - Agreements are normally held by the dealer for 12 months and not by the CSP. They are then securely destroyed.
- Internet/Email
 - Details held will vary dependent on whether it is a free services e.g MickeyMouse@Hotmail.com , or a Voice Over Internet Service Protocol VOIP e.g Skype and a paid for service e.g Nadine@aol.com or broadband where the company should have my name, address and payment details..

When Can I Spy on people

- **Covert surveillance, as used by Public authorities under Part II of the Regulation of Investigatory Powers Act 2000, falls within two categories; Directed surveillance or intrusive surveillance.**
- **Definition of directed surveillance**
- This is defined in section 26(2) of the 2000 Act as surveillance which is covert, but not intrusive, and undertaken:
 - for the purposes of a specific investigation/operation
 - in such a manner as is likely to result in the obtaining of private information about a person
 - It would not be reasonably practicable BUT FOR an authorisation under Part II of the 2000 Act to gain access to the information sought.
 - Directed surveillance can only be carried out by those public authorities who are listed in Part I and Part II of schedule 1 of the 2000 Act.

When Can I Spy on people



- **Definition of intrusive surveillance**
- is defined in section 26(3) of the 2000 Act as covert surveillance that:
 - is carried out in relation to anything taking place on any residential premises or in any private vehicle
- involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device.
- Applications to carry out intrusive surveillance can only be made by the senior authorising officer of those public authorities listed in or added to section 32(6) of the 2000 Act .
- Intrusive Surveillance can only be conducted for the purpose of SERIOUS Crime, National Security or the Interest of Economic Well-Being of the UK

What is a SPoC?



- The single point of contact (SPoC) is either an accredited individual or a group of accredited individuals **trained** to facilitate lawful acquisition of communications data and effective co-operation between a public authority and CSPs.

Ministerial Comment

What is a SPoC?

- A SPOC promotes efficiency and good practice in ensuring only practical and lawful requirements for communication data are undertaken.
- The SPOC also provides objective judgement and advice to both the applicant and the designated person.
- The SPOC provides a guardian and gatekeeper function ensuring that public authorities act in an informed and lawful manner.



Home Office
BUILDING A SAFE, JUST
AND TOLERANT SOCIETY

Promotes efficiency and good practice in **ensuring only practical and lawful requirements for communications data are undertaken**. This encourages the public authority to regulate itself. The SPoC provides objective judgement and advice to both the applicant and the designated person. In this way the **SPoC provides a "guardian and gatekeeper" function ensuring that public authorities act in an informed and lawful manner.**

Ministerial
Comment

SPOC considerations

- The SPOC should therefore be in a position to:
 - Assess whether the acquisition of specific communications data from a CSP is reasonably practical.....
 - Provide assurance to designated persons that authorisations and notices are lawful under the Act and free from errors.....



Home Office
BUILDING A SAFE, JUST
AND TOLERANT SOCIETY

Do we need a SPoC?

- Public authorities unable to call upon the services of an accredited SPoC should not undertake the acquisition of communications data.

Ministerial Comment

What is an SRO?

- Senior Responsible Officer **must** be responsible for:
- the integrity of the process in place within the public authority to acquire communications data;
- compliance with Chapter II of Part I of the Act and with this code, and
- oversight of the reporting of errors to the Commissioner and the identification of both the cause(s) of errors and the implementation of processes to minimise repetition of reported errors

Ministerial Comment

Does it matter, all this SPoC & SRO stuff?



- Should the Commissioner establish that an individual has been adversely affected by any wilful or reckless failure by any person within a relevant public authority exercising or complying with the powers and duties under the Act in relation to the acquisition or disclosure of communications data, he shall inform the affected individual of the existence of the Tribunal and its role. The Commissioner should disclose sufficient information to the affected individual to enable him or her to effectively engage the Tribunal.

Ministerial Comment

Is The Request feasible?

- Many organisations now offer telephone and internet services the SPoC needs to make themselves familiar with who offers what.
- All CSPs have their own systems, capabilities and differing retention periods.
- As the SPOC you need to be aware of a CSPs capability in order to identify whether a request is feasible or not.
- It is impossible for anyone to know everything about every single CSP.



Is it feasible?

- There are many tools that can assist them in this task



- Identification of telephone network – use a tool such as

- <http://www.magsys.co.uk/telecom/codelook.asp>

• However, don't forget about number portability and 'virtual networks' such as Virgin Mobile who run off the T-Mobile (UK) network.



- Most telcos sell airtime/minutes to a number of wholesale partners but you will not be able to identify this from a code look up site.



Home Office
BUILDING A SAFE, JUST
AND TOLERANT SOCIETY



Is it feasible?

• Knowing whether a request is feasible as RIPA request issued to an incorrect CSP means delays as well as a reportable error:

• Here is a little help.....



**07962 400000 -
499999**



07963, 07986, 07905, 07913,
07941, 07952, 07906, 07981,
07910, 07914, 07722, 07804,
07758



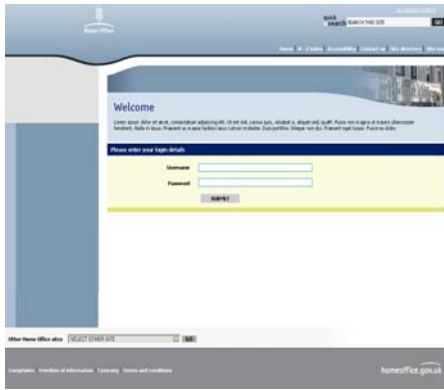
07962 00000 - 07962 399999

• A Wholesale partner will normally 'own' the customer detail, whilst The owner of the network holds traffic data information. *



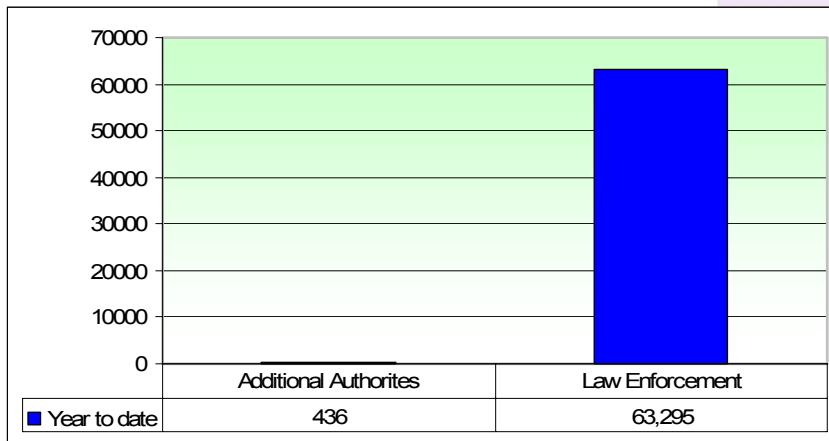
Home Office
BUILDING A SAFE, JUST
AND TOLERANT SOCIETY

Is it feasible?



<http://ripa.homeoffice.gov.uk>

Volume of requests – Additional Authorities and Law Enforcement



For 1 CSP in 2005

Grading

- In order to prioritise requests on a national basis, the ACPO Data Communications Group have agreed a grading table for all applications received by a CSP. These are currently under review
- Grade 1 – for the purpose in an emergency of preventing an immediate threat to human life;
- Grade 2 – Arrests for SERIOUS CRIMES planned within next 24 hours, or taking place of prisoners in custody and data is required to secure a charge where releasing suspect not in public interest;
- Grade 3 – response to an investigation into a human death where that enquiry has commenced within last 14 days.



Home Office
BUILDING A SAFE, JUST
AND TOLERANT SOCIETY

Grading

- Grade 4 – investigation into SERIOUS CRIME or where the data is required for court where a court date has been set or in order to meet a deadline set under Section 51 of Crime and Disorder Act 1998
- Grade 5 – All other enquiries



Home Office
BUILDING A SAFE, JUST
AND TOLERANT SOCIETY

Service Level Agreements



- RIPA does not impose any time limits on responses from a CSP. The Home Office is currently reviewing whether there should be formal SLAs with CSPs
- However, most CSPs will have put in place their own SLAs (Service Level Agreement) with relation to responses according to grading.
- Most CSPs work on the following timescales with relation to manual requests (Notices.)
 - Grade 1 – Within an hour
 - Grades 2 & 3 – Within 24 – 48 hours
 - Grades 4 & 5 – Within 10 working days

RIPA Application - Practical Examples



- **Dumping Top Soil** - We have receive an allegation for example that a company is exporting topsoil from a landfill site contrary to a planning condition. No criminal offence has been committed, only a breach of a condition.
 - How do we obtain the evidence?
 - Can we use RIPA once a Notice has been breached?
- **Repairs At A Residential Premises** - we have received an allegation that someone is carrying out car repairs at a residential property.
 - Can we do drive bys?
 - When is it appropriate to use RIPA?
- **We want to Use A Model Airplane** – Can we use a model airplane for the videoing of landfill sites, or any other breach of planning control/enforcement notice?
- **Used As A Church** - The use of a residential property, subject of a valid Enforcement Notice to cease the use as a place of worship. Allegations that it was being used at times like Ramadan, chanting heard coming from property

RIPA Application - Practical Examples



Home Office
BUILDING A SAFE, JUST
AND TOLERANT SOCIETY

- Drive by/Airplanes – Car/Landfill site has no private life
- Valid Enforcement Notice - when a notice is breached then a crime has been committed, as long as it is your intention to prosecute then RIPA can be used to PREVENT & DETECT CRIME (28 (3) (b)).
- Remember the action needs to be proportionate to what is aimed to be achieved by the action – Do not take a sledge hammer to crack a nut sometimes knocking on the door and asking works better.
- RIPA is about preventing and detecting crime not workplace monitoring e.g. accessing staff phone bills and internet records. Should be covered by workplace policy.

Remember



Home Office
BUILDING A SAFE, JUST
AND TOLERANT SOCIETY

- Activity is monitored by the oversight regime (OSC & ICCO)
- All such activity should be carefully managed to meet the objective in question and must not be arbitrary or unfair. If a person believes that their rights have been interfered with unlawfully they can complain to the Investigatory Powers Tribunal
- RIPA Codes of Practice source of guidance
- Help can be obtained from the Home Office 0207 035 1220
<http://security.homeoffice.gov.uk/> or LACORS (0)20 7840 7200
www.lacors.gov.uk



Home Office
BUILDING A SAFE, JUST
AND TOLERANT SOCIETY

Nadine Hibbert

**Covert Investigation Policy Team
Crime Reduction and Community Safety Group
Home Office**

 **020 7035 1208**

 **nadine.hibbert@homeoffice.gsi.gov.uk**



Home Office

BUILDING A SAFE, JUST
AND TOLERANT SOCIETY