Personal, Professional, Protective Policing

FREEDOM OF INFORMATION REQUEST

Request Number: F-2011-03422

Keyword: Crime

Subject: RIPA Communications Data

Request and Answer:

Questions

1. How many applications have been made to access communications data under Chapter II of Part I of RIPA in each of the past five years?
2. How many of these applications have been granted in each of the past five years?
3. How many individuals' data did these requests encompass in each of the past five years?
4. How much have you spent on accessing customer communications data from:
   Mobile phone companies in each of the past five years
   Internet service providers in each of the past five years
   Landline phone companies in each of the past five years
   I would like to receive the information in electronic format, as a CSV file or spreadsheet.

Please let me know at your earliest convenience if you require any clarification with this request.

If my request is denied in whole or in part, I ask that you justify all deletions by reference to specific exemptions from the act. I also ask that you release all non-exempt material, even if some material is found to be exempt.

I would be grateful if you could confirm in writing that you have received this request, and look forward to your response within 20 working days, as outlined in the statute

I am writing to confirm that the Police Service of Northern Ireland has now completed its search for the information.

Answer 1

Total Applications, from 1st January to 31st December by year:

2007 - 2402

2008 - 2234

2009 - 3256

2010 - 3556

2011 – 31/10/01/01/2011 ~ 17/10/2011.

Answer 2
How many of these applications have been granted in each of the past five years?

From 1st January to 31st December by year:

2007 - Granted 2289

2008 - Granted 2131

2009 - Granted 3077

2010 - Granted 3385

2011 - Granted 2869 01/01/2011 ~ 17/10/2011.

Answer 3
How many individuals' data did these requests encompass in each of the past five years?

The PSNI systems do not record the number of applications against individuals, only how many applications as a whole where applied for, to access communications data under Chapter II of Part I of RIPA (As at answer 1).

Additionally the Police Service of Northern Ireland can Neither Confirm Nor Deny (NCND) any other information is held relevant to your request.

Section 17(1) of the Freedom of Information Act 2000 requires the Police Service of Northern Ireland, when refusing to provide any further information to provide you the applicant with a notice which:

(a) states that fact,
(b) specifies the exemption in question and
(c) states (if not otherwise apparent) why the exemption applies.

Section 23(5) Information relating to the Security bodies;
Section 24(2) National Security;
Section 30(3) Investigations;
Section 31(3) Law enforcement;

This should not be taken as conclusive evidence that any information that would meet your request exists or does not exist.

Section 23 (5) is an absolute exemption and I am not required to provide a Public Interest Test or a Harm Test.

Sections 24 (2) and 31(3) are prejudice based qualified exemptions and there is a requirement to articulate the harm that would be caused in confirming or not that the information is held as well as carrying out a public interest test.

Section 30 (3) is a qualified class-based exemption and there is a requirement to conduct a public interest test.

Overall harm for partial NCND

In order to counter criminal and terrorist behaviour it is vital that the police and other agencies have the ability to work together, where necessary covertly, in order to obtain intelligence within current legislative frameworks to ensure the successful arrest and prosecution of those who commit or plan to commit acts of terrorism. In order to achieve this goal, it is vitally important that information sharing takes place with other police forces and security bodies within the UK and Internationally in order to support counter-terrorism measures in the fight to deprive international terrorist networks of their ability to commit crime.

It should be recognised that the international security landscape is increasingly complex and unpredictable. The UK faces a serious and sustained threat from violent extremists and this threat is greater in scale and ambition than any of the terrorist threats in the past.

Since 2006, the UK Government have published the threat level, based upon current intelligence and that threat has remained at the second highest level, 'severe', except for two short periods during August 2006 and June and July 2007, when it was raised to the highest threat 'critical'.

The Police Service is committed to demonstrating proportionality and accountability regarding surveillance techniques to the appropriate authorities. However, if the Police Service were to either confirm or deny that any other information exists; other covert surveillance tactics will either be compromised or significantly weakened. If the Police Service denies a tactic is used in one request but then exempts for another, requesters can determine the 'exempt' answer is in fact a technique used in policing. The impact could undermine national security, any on-going investigations and any future investigations, as it would enable targeted individuals/groups to become surveillance aware. This would help subjects avoid detection, and inhibit the prevention and detection of crime.

The prevention and detection of crime is the foundation upon which policing is built and the police have a clear responsibility to prevent crime and arrest those responsible for committing crime or those that plan to commit crime. To do this the police require evidence and that evidence can come from a number of sources, some of which is obtained through covert means. Having obtained sufficient evidence offenders are charged with offences and placed before the courts. By confirming or denying that any other information pertinent to this request exists could directly influence the stages of that process, and jeopardise current investigations or prejudice law enforcement.

Any information identifying the focus of policing activity could be used to the advantage of terrorists or criminal organisations. Information that undermines the operational integrity of these activities will adversely affect public safety and have a negative impact on both national security and law enforcement.

Public Interest Test

Factors favouring confirmation or denial for S24

The public are entitled to know how public funds are spent and by confirming or denying that any other information relevant to the request exists could lead to a better-informed public that can take steps to protect themselves.

Factors against confirmation or denial for S24

By confirming or denying that any other information relevant to the request exists would render Security measures less effective. This could lead to the compromise of ongoing or future operations to protect the security or infra-structure of the UK and increase the risk of harm to the public.

Factors favouring confirmation or denial for S31

By confirming or denying that any other information relevant to the request exists, would enable the public to see where public funds are being spent. Better public awareness may reduce crime or lead to more information from the public.

Factors against confirmation or denial for S31
By confirming or denying that any other information relevant to the request exists, law enforcement tactics could be compromised which could hinder the prevention and detection of crime. More crime could be committed and individuals placed at risk.

Factors favouring confirmation or denial for S30
By confirming or denying that any other information relevant to the request exists would enable the public to obtain satisfaction that all investigations are conducted properly and that their public money is well spent.

Factors against confirmation or denial for S30
By confirming or denying that any other information relevant to the request exists, would hinder the prevention or detection of crime, undermine the partnership approach to law enforcement, which would subsequently affect the PSNI's future law enforcement capabilities.

Balance test
The security of the country is of paramount importance and the Police Service will not divulge whether information is or is not held if to do so could undermine National Security or compromise law enforcement. Whilst there is a public interest in the transparency of policing operations and in this case providing assurance that the police service is appropriately and effectively engaging with the threat posed by the criminal fraternity, there is a very strong public interest in safeguarding both national security and the integrity of police investigations and operations in this area.

As much as there is public interest in knowing that policing activity is appropriate and balanced in matters of national security this will only be overridden in exceptional circumstances. Therefore it is our opinion that for these issues the balancing test for confirming or denying whether any other information relevant to your request exists is not made out.

There is also no requirement to satisfy any public concern over the legality of police operations and the tactics we may or may not use. The PSNI is already held to account by independent bodies such as The Office of the Surveillance Commissioner and The 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 containing statistical information. Our accountability is therefore not enhanced by confirming or denying that any other information is held.

None of the above can be viewed as an inference that any other information does or does not exist.

Answer 4
How much have you spent on accessing customer communications data from:
Mobile phone companies in each of the past five years?
Internet service providers in each of the past five years?
Landline phone companies in each of the past five years?

Below are the totals spent on gaining communications data under Chapter II of Part I of RIPA:-

- Year 06/07 spent £312,304.18 including VAT on all communications data received.
- Year 07/08 spent £176,694.86 including VAT on all communications data received.
- Year 08/09 spent £167,670.75 including VAT on all communications data received.

- Year 09/10 spent £236,246.96 including VAT on all communications data received.
- Year 10/11 spent £182,600.31 including VAT on all communications data received.
- Year 11/12 to 17th Oct 2011 spent £82,015.66 including VAT on all communications data received.

Harm
No breakdown can be given as to the number of applications applied for or money spent on Communications Service Provider's (CSP) or type of CSP. The disclosure of this information could adversely impact the communication company's business, by highlighting how often law enforcement agencies are making requests from them, which may lead to their customers or potential customers moving to another provider, based on this information.

Some companies have bespoke systems to accommodate the disclosure of data via a secure system to enable virtual 'real-time' collection by the police and those systems need to be funded through cost recovery.

To disclose the actual breakdown of costs by these companies would reveal an inaccurate 'skewing' of the cost recovery statistics as CSPs who have built bespoke systems provide more services than CSPs who do not. Any misinterpretation by individuals may result in certain CSPs being branded as 'the criminal's choice' which would damage the working relationship between the police, CSPs and the Government.

With this relationship impeded, a CSP may pull their services without prior notice which would compromise the prevention and detection of crime.

Disclosure would also reveal which CSPs are limited in their abilities and those which have the better capabilities, potentially giving a tactical advantage to criminals who would choose networks based on risk.

A total breakdown of charges would reveal the services provided by CSPs, which would include covert services. Any such disclosure would provide the full inabilities and capabilities of each CSP which in turn would benefit a terrorist or criminal by revealing what services and systems are used by the Police Service. This awareness would enable members of the criminal fraternity to take evasive steps to avoid detection.

The above harm engages Section 43 and Section 31.

Section 43(2) Commercial Interests is a prejudiced based Qualified exemption and as such requires the harm to the evidenced and a public interest test to be carried out.

Section 31(1) (a) (b) Law Enforcement is also a prejudice based Qualified exemption which requires the prejudice (harm) to be evidenced and a public interest test to be carried out.

Public Interest Test
Section 31(1) (a) (b)
<u>Considerations favouring Disclosure</u>
When information disclosed relates directly to the efficiency and effectiveness of the PSNI or its officers it is generally of benefit to the community. In this case, the release of information will enable the public to have a better understanding of the efficiency and effectiveness of the police service.

<u>Considerations favouring Non-Disclosure</u>
Where a current or future Law enforcement role of PSNI may be compromised by the release of information. In this case, disclosure of the information may enable individuals or terrorist organisations to identify expert technology and methods used by the police service as part of an intelligence gathering operation. The effectiveness of current and future strategies to combat terrorist

activity may be compromised and may also inhibit the ability to prevent crime.

Section 43(2)

Considerations favouring Disclosure

One of the underlying principles of the Freedom of Information Act is the need for authorities to be more open and transparent. In this case, to provide the full detail of costings for telephony data would provide the community with an awareness that public funds are being used to resource and finance the use of expert technology to assist in the prevention or detective of crime and the apprehension or prosecution of offenders.

Considerations favouring Non-Disclosure

Although the request does not ask for personal information the interests of third parties, i.e. the Communication Service Providers, is compromised. The Police Service has a moral duty to protect the sensitive commercial information it holds about any private company they have dealings with. In this case, to provide the fine detail of how much the companies charge would prejudice the commercial interests of those companies, as detailed within the harm above.

The charge a private company makes for their services is an individual agreement between the CSP and the Force/Service. To provide costing details would undermine the company in its ability to be competitive when providing services to the public sector. Any such disclosure would compromise that company's pricing structures which would leave them vulnerable to unfair negotiations when a customer requires their services.

Balancing Test

When balancing the public interest test we have to consider whether the information should be released into the public domain. Arguments need to be weighed against each other. The most persuasive reason for disclosure is Use of Public Funds which needs to be compared to the strongest negative reason, which in this case is Public Safety. The police service cannot and will not disclose information which will place the public at risk by undermining national security or law enforcement thereby assisting those intent on committing crime.

Information released under FOIA, where exemptions apply, will only be done where there is a tangible community benefit which is more powerful than the harm that could be done. This does not apply in this case.

On balance, and from the harm evidenced above, the information requested should be protected and exemptions applied.

If you have any queries regarding your request or the decision please do not hesitate to contact me on 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.