BIG BROTHER WATCH

Police Access to Communications Data

How UK Police Forces requested access to communications data over 700,000 times in 3 years.

A Big Brother Watch Report

June 2015

Contents

Executive Summary

Communications Data details the who, where and when of any text, email, phone call or web search. Law enforcement regularly state that Communications Data have become an essential tool in criminal investigations. The intrusive nature of Communications Data however has ensured that it is now a highly contentious political, legal and policing issue in the UK and around the world.

Police Access to Communications Data is part of Big Brother Watch's ongoing call for greater transparency for the use of our personal data. Focusing on the use of Communications Data by police forces, this report shows that between 2012 and 2014, **733,237 requests for Communications Data were made.** The equivalent of **670 requests a day or 28 requests every hour.**

Despite persistent claims that the police's access to Communications Data is diminishing, this report shows that the police are continuing to access vast amounts of data on citizens. Indeed, this report shows that **on average 96% of all requests are internally approved with an average of only 4% being refused.** Claims of a 25% capability gap - the gap between the amount of Communications Data created and the ability for the police to access it - are therefore clearly overstated.

It is clear from the reports' findings that disparity exists amongst police forces on what is considered necessary and proportionate for a request for Communications Data and why a refusal for access is given. If law enforcement persists with calls for greater access, internal procedures will need to be clarified, transparency about the process published and independent judicial approval brought in as part of the authorisation process.

As a result of these findings, Big Brother Watch remain concerned about the excessive access and use of Communications Data. We propose a number of recommendations which would increase transparency, encourage better safeguards and create a clearer application process.

Recommendations:

1. Police forces should be required to publish transparency reports detailing how requests are approved, the number of individuals affected and the type of crime Communications Data is used for.
2. Proof that data of more than 6 months old is regularly used in order to establish a proportionate approach to data retention.
3. A clear, standardised procedure for the access of Communications Data, which all police forces, telecommunications and internet service providers must adhere to.

4. Judicial approval should be the final step in any request for Communications Data.
5. New definitions for Communications Data should be adopted.

Should the government adopt these recommendations, the general public will be better informed about how their communications can be obtained, analysed and used. It will also provide the much needed clarity on how police and other organisations work with the technology companies to access this information.

Key Findings

All figures are for 1st January 2012-31st December 2014 unless otherwise stated. A table of all police forces and a breakdown of their requests, rejections and approvals is available on p.15.

- There have been **733,237** applications to access Communications Data by police forces. This is equivalent to:
    - **244,412** requests every year.
    - **20,368** requests every month.
    - **4,700** requests every week.
    - **670** requests every day.
    - **28** requests every hour.
    - **1** request every **2 minutes**
- Of this total figure:
    - **679,073** of the requests were granted internally
    - Meaning that **54,164** of were rejected.
- On average **96% of all requests are approved, with just 1 in 25 (4%) of requests being rejected**.
- Across police forces that could provide yearly breakdowns:
    - **26 showed increasing** numbers of requests.
    - **11 showed falling numbers**.

Table 1: Highest number of Requests for Communications Data

No.	Force	No. of Requests
1	Metropolitan Police	177,287
2	West Midlands Police	99,444[1]
3	Police Scotland	62,075
4	Northumbria Police	21,345
5	West Yorkshire Police	19,757
6	Devon and Cornwall Police	19,731
7	Essex Police	19,541
8	Greater Manchester Police	19,037
9	Avon and Somerset Constabulary	18,923
10	Thames Valley Police	17,562

Table 2: Highest number of Refusals

This table shows the police forces that have had the highest number of refused requests. The percentage of the requests submitted and the refusals received is also included.

The average refusals for police forces is 4.1%

No.	Force	No of Requests	No. of Refusals	Percentage Refused
1	Essex Police	19,541	5,560	28%
2	Kent Police	15,566	3,715	23%
3	Metropolitan Police	177,287	32,879	18%
4	North Yorkshire Police	3609	496	13%
5	Police Service of Northern Ireland	15,166	1,079	7.1%
6	Derbyshire Constabulary	4,406	272	6.1%
7	Merseyside Police	12,746	731	5.7%
8	Avon and Somerset Constabulary	18,923	904	4.8%
9	Cambridgeshire Constabulary	2,385	114	4.7
10	Northamptonshire Police	3,374	148	4.3%

[1] Total refers to the "*Total number of Notices and Authorisations to acquire communications data under Part I Chapter II of the Regulation of Investigatory Powers Act (RIPA)*."

Table 3: Lowest number of Refusals

This table shows the police forces that have had the lowest number of refused requests. The percentage of the requests submitted and the refusals received is also included.

No.	Force	No. of Requests	No. of Refusals	Percentage Refused
1	Cheshire Constabulary[2]	5,848	7	0.1%
2	Warwickshire Police	1,807	4	0.2%
3	Cleveland Police	4,276	14	0.3%
3	Northumbria Police	21,345	54	0.3%
4	Hertfordshire Constabulary	13,914	58	0.4%
5	British Transport Police	3,539	16	0.5%
6	Durham Constabulary	6,812	41	0.6%
7	Cumbria Constabulary	9,805	74	0.8%
7	West Mercia Police	11,233	88	0.8%
8	Leicestershire Police	9,438	87	0.9%
8	South Wales Police	2,801	24	0.9%
9	Gwent Police	12,449	119	1%
10	Police Scotland	62,075	1,080	1.7%

[2] This figure refers to *work flow packages*". It adds that "*Each work flow package can contain anything up to 40 separate requests*".

Policy Recommendations

1. **Police forces should be required to publish transparency reports detailing how requests are approved, the number of individuals affected and the type of crime Communications Data is used for.**

Police forces and other organisations, such as the National Crime Agency and the intelligence agencies that use Communications Data should be required to publish annual transparency reports detailing how data is accessed, the number of people affected and a clear breakdown of the type of crime for which all Communications Data requests are made.

Currently, if the public want to know about how their communications can be accessed by law enforcement, their only source of information is from the transparency reports published by a handful of technology companies. It is unacceptable that law enforcement agencies that access and use our personal data are so lacking in transparency and are so reluctant to express the purpose and process of this element of policing.

A statistical analysis of how often these powers are requested, how often they are refused and how effective they are when used, would assist in increasing public understanding of why Communications Data plays a crucial role in 21st century policing.

A requirement to publish this information in an easily accessible and understandable format would ensure that the agencies would adhere to strict record keeping processes and establish a uniform procedure for requesting data, working with communications companies in a standardised format and establishing a clear data trail. This should help combat the disparity of the approval/refusal process which our data reveals is occurring amongst police forces.

The publication of this information should not be left to the Interception of Communications Commissioner's Office (IOCCO). This would risk turning the IOCCO into a statistical bulletin, when their focus should be on commenting on the legality and robustness of the actions revealed.

2. **Proof that data of more than 6 months old is regularly used in order to establish a proportionate approach to data retention.**

Transparency reports should include detail on how long the data has been held for prior to a request being made by law enforcement. In light of the Data Retention and Investigatory Powers Act 2014 (DRIPA) clarity is required to understand whether data under 6 months old is used more frequently than data exceeding 6 months. This would further assist in the debate on these powers. This is of particular importance in light of DRIPA's December 2016 sunset clause.

3. **A clear, standardised procedure for the access of Communications Data which all police forces, telecommunications and internet service providers must adhere to.**

There are currently three ways in which law enforcement are able to request data from telecommunications and internet service providers:

- Direct request to the company
- Emergency procedure for use purely when there is a threat to life
- Through a Mutual Legal Assistance Treaty (MLAT), issued from government to government.

Whilst many of the larger telecommunications and internet service providers have departments purely to assist with requests, smaller companies are less likely to have a standardised procedure or team of specialists on hand. It is critical that there is a standardised and regulated process which law enforcement and the companies, regardless of size, know to follow. This should ensure that there is no room for error, confusion or time delays in urgent cases.

4. **Judicial approval should be the final step in any request for Communications Data.**

If an organisation wants to access Communications Data it should, as a final step, obtain approval from a national independent judicial body.

Currently the system culminates with the sign-off from an internal Single Point of Contact (SPoC). Whilst law enforcement have worked hard at promoting the benefit of the internal SPoC system, based on the findings of our report and the sheer volume of communications data requests approved, we believe that a further independent level of approval is necessary to ensure that a standardised procedure exists across all police forces.

This system would ensure an independent assessment of the necessity and proportionality of the request. It would act as an extra safeguard. Should a problem occur during an investigation external approval will be of benefit in ensuring that independence was maintained whenever a request for personal data was made.

Concerns regarding time constraints which further oversight may bring we believe are unfounded. The creation of a specialist system able to receive and respond to requests quickly and efficiently 24/7 would ensure that a trained, specialised legal figure would be on hand whenever a request was made to offer completely independent oversight. This would create a further level of reassurance for law enforcement that their request is valid.

5. New definitions for Communications Data should be adopted.

The current definition of Communications Data bundles a broad range of information under a single category.

The Intelligence and Security Committee's 2015 report *Privacy and Security: A modern and transparent legal framework* acknowledged this as a concern and recommended that more intrusive elements of Communications Data be re-defined as *'Communications Data Plus'* and other information, such as the accent of a speaker, as *'Content Derived Information'*.[3]

They recommended that *'Communications Data Plus'* be granted additional safeguards whilst *'Content Derived Information'* would be subject to the same protections as intercepted content of a message.[4]

This would provide additional clarity and is a sensible recommendation that should be adopted into any new legislation.

---

[3] Intelligence and Security Committee, Privacy and Security: A modern and transparent legal framework, 12th March 2015, p. 53: https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20150312_ISC_P%2BS%2BRpt%28web%29.pdf?attachauth=ANoY7cqLKesyC8EvkWtAIyEeM1P6Caya1Eg9Y31l4fVTE9MUrtDF6ioZe1_97BbSeXKcTnR-X_c2J6zjKXEBXlf_zB2co_wjJ8nUmGldw5hrhl61tZKhhf7kXFvAkwcdckE_GrGda35osPgM4s_0KVCAB92gulMu_HaUJ8_EOJgyvZagJjy8J3Go0mCexYZL_aL0Z_FlodlWXqAt38can2ANyIYPRCmCobImx7l8OWpzihAx133h9lDjcOMTI6VND1WXx2RzexR2&attredirects=0

[4] Intelligence and Security Committee, Privacy and Security: A modern and transparent legal framework, 12th March 2015, p. 53: https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20150312_ISC_P%2BS%2BRpt%28web%29.pdf?attachauth=ANoY7cqLKesyC8EvkWtAIyEeM1P6Caya1Eg9Y31l4fVTE9MUrtDF6ioZe1_97BbSeXKcTnR-X_c2J6zjKXEBXlf_zB2co_wjJ8nUmGldw5hrhl61tZKhhf7kXFvAkwcdckE_GrGda35osPgM4s_0KVCAB92gulMu_HaUJ8_EOJgyvZagJjy8J3Go0mCexYZL_aL0Z_FlodlWXqAt38can2ANyIYPRCmCobImx7l8OWpzihAx133h9lDjcOMTI6VND1WXx2RzexR2&attredirects=0

What is Communications Data?

How Are Communications Data Used?

We understand that Communications Data are an important tool for law enforcement and the security agencies and are widely used during investigations.

The Home Secretary, Theresa May MP, commented that "*communications data has played a significant role in every Security Service counter-terrorism operation in the last decade*".[5]

Sir Jonathan Evans, former Director General of MI5, echoed this sentiment, arguing that there "*are no significant investigations that we undertake across the service that don't use communications data*".[6]

The Home Office's impact assessment which accompanied DRIPA cited murder, sexual exploitation and door step fraud, as crimes which would be "*harder or impossible*" to investigate without the proper access to Communications Data. It also highlighted the importance of Communications Data's in locating missing persons.[7]

Are Communications Data Intrusive?

The public is repeatedly told that Communications Data are simply the who, what, where and when of a communication and are therefore not as intrusive as the content of a message.

Yet that information can paint a vivid and intrusive picture of our lives, including who our friends, family and work colleagues are, where we travel, live, work, socialise and holiday, and the websites we visit online. Communications Data can include:

- Who we call, text or email
- Our location using the GPS of our mobile telephone or the IP address of our home computer.
- The method of communication we use
- The websites we visit

---

[5] T. May, *Speech to RUSI: Home Secretary Theresa May on counter-terrorism*, 24th November 2014: https://www.gov.uk/government/speeches/home-secretary-theresa-may-on-counter-terrorism

[6] Intelligence and Security Committee, *Access to communications data by the intelligence and security Agencies*, February 2013, p. 9: https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20130205_ISC_CD_Report.pdf?attachauth=ANoY7coDAMcUdPloI0gFSWEMzI24vXdOunxALyJ8y3Xiu85Jtsf_wZ0t6Xeab7tBQpryfSpp9xFszP1I_e85odnithSawJZQQeLuRlKjXTJhMmB7lwdOVxfGcdva57kJNdfw1_O0FGCrjvnk1E9LIpz1AqaPTrh7jwAsa4u4reSScsnpb3brg6_aPk6-Mkv5p8FJDMxsN0eWM9hkWIBy4G8qMIbHCf-e-ukGM8n5ZbcQxRJFqV7mHt4%3D&attredirects=0

[7] Home Office, *Impact Assessment: Data Retention Legislation*, 27th June 2014, p. 5: http://www.parliament.uk/documents/impact-assessments/IA14-15A.pdf

This level of detail has led to some, including Edward W. Felton, Professor of Computer Science and Public Affairs at Princeton University to comment that "*it is no longer safe to assume that this "summary" or non-content" information is less revealing or less sensitive than the content it describes*."[8]

Communications Data are also known as "*metadata*". Metadata is viewed as highly controversial. Speaking about its value, the former head of the CIA Michael Hayden stated that "*we kill people based on metadata*".[9]

The Intelligence and Security Committee's 2015 report highlighted that certain aspects of Communications Data "*have the potential to reveal details about a person's private life that are more intrusive* [than conventional Communications Data]"[10]

The Information Commissioner's Office has argued that Communications Data "*can be very revealing and intrusive in a wide range of contexts*".[11]

Is there a Capability Gap?

During the debate regarding Communications Data in 2013, we heard many political claims that there is a "capability gap" between the amount of communications being created and the amount which are accessible to law enforcement.

The Intelligence and Security Committee's 2013 report *Access to Communications Data by the Intelligence and Security Agencies* quoted a Home Office estimate which put the potential gap at around 25%.[12]

---

[8] E. Felton, *Written Testimony of Edward W. Felton to US Senate, Committee on the Hearing on Continued Oversight of the Foreign Intelligence Surveillance Act*, 2nd October 2013: http://www.cs.princeton.edu/~felten/testimony-2013-10-02.pdf?

[9] Wired, NSA Doesn't Need to Spy on Your Calls to Learn Your Secrets, 25th March 2015: http://www.wired.com/2015/03/data-and-goliath-nsa-metadata-spying-your-secrets/

[10] Intelligence and Security Committee, Privacy and Security: A modern and transparent legal framework, 12th March 2015, p. 6: https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20150312_ISC_P%2BS%2BRpt%28web%29.pdf?attachauth=ANoY7cqLKesyC8EvkWtAIyEeM1P6Caya1Eg9Y31l4fVTE9MUrtDF6ioZe1_97BbSeXKcTnR-X_c2J6zjKXEBXlf_zB2co_wjJ8nUmGldw5hrhl61tZKhhf7kXFvAkwcdckE_GrGda35osPgM4s_0KVCAB92gulMu_HaUJ8_EOJgyvZagJjy8J3Go0mCexYZL_aL0Z_FlodlWXqAt38can2ANyIYPRCmCobImx7l8OWpzihAx133h9lDjcOMTI6VND1WXx2RzexR2&attredirects=0

[11] Information Commissioners Office, *submission to the Intelligence and Security Committee of Parliament*, p. 7: https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/public-evidence/12march2015/20150312-P%2BS-004%20-Information%20Commissioner.pdf?attachauth=ANoY7crW9DfIO6ZuQQ9t0LucfrvC5HwnMeQZRiYriXCa5r94HYYsQV7DpGwxseoKBSmpTMVWwgbwvj4-iHsMOn9d5EEhuicAP9R_uzy4bOjxdn0wlpPas7bkLb5LLL1Bsn1Uhs0sbt_BNNVKrcGbhzMBXzSnVAL4bqI4qjSnAZC5B7AT0EADbrFICFBlVuQVj1foQdRcsWg_X92Taf6doQtqC7iu_vhwgzWBRxYDjhqprQPhBxSGUF5qPChauZtSV3aTQ9A-2yW5FFeoTCK58D9w1cdVebps20CXL5wGV_fr0iugAIH-tKA%3D&attredirects=0

[12] Intelligence and Security Committee, *Access to communications data by the intelligence and security Agencies*, February 2013, p. 11: https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20130205_ISC_CD_Report.pdf?attachauth=ANoY7coDAMcUdPloI0

This figure has never been proven. During an Intelligence and Security Committee evidence session, Sir Jonathan Evans, then the Director General of MI5, also questioned the veracity of the figure, arguing that it rested on "*some pretty heroic assumptions*."

The Joint Committee on the Draft Communications Data Bill has argued that part of the capability gap was down to a "*lack of ability of law enforcement agencies to make effective use of the data that is available*"[13] and that the figure was "*an unhelpful and potentially misleading figure*"[14]

This report shows that the vast majority of requests made by police forces are approved, with the average percentage refusals being 4%, potentially giving law enforcement access to a vast amount of information.

When you compare the figures in this report with the evidence provided by US technology companies in their annual transparency reports, it shows that when they receive a request it is, in the overwhelming majority of cases, complied with. It is critical therefore that a standardised understanding of what defines necessary and proportionate is applied.

Using Facebook as an example, their report shows that the number of requests that were rejected has gone down – 29% being rejected in Jan-Jun 2013 compared to 25% in Jul-Dec 2014.[15] [16] Commenting on when requests are rejected, Facebook said:

> "*We respond to valid requests relating to criminal cases. Each and every request we receive is checked for legal sufficiency and we reject or require greater specificity on requests that are overly broad or vague*."

This would echo the comments made by the Joint Committee on the Draft Communications Data Bill.

Similarly research by the NSPCC found that although police forces often seize hundreds of computers each year, they lack the resources to properly investigate what data is held on them.[17] This is a clear example that access to the data is not the problem, but the lack of resources and manpower to effectively deal with the demand.

---

gFSWEMzI24vXdOunxALyJ8y3Xiu85Jtsf_wZ0t6Xeab7tBQpryfSpp9xFszP1I_e85odnithSawJZQQeLuRlKjXTJhMmB7IwdOVxfGcdva57kJNdfw1_O0FGCrjvnk1E9LIpz1AqaPTrh7jwAsa4u4reSScsnpb3brg6_aPk6-Mkv5p8FJDMxsN0eWM9hkWlBy4G8qMIbHCf-e-ukGM8n5ZbcQxRJFqV7mHt4%3D&attredirects=0

[13] Joint Committee on the Draft Communications Data Bill, Draft Communications Data Bill, 28th February 2012, p. 16: http://www.publications.parliament.uk/pa/jt201213/jtselect/jtdraftcomuni/79/79.pdf

[14] Ibid, p. 16

[15] Facebook, *Global Government Requests Report*: July 2013-December 2013, https://govtrequests.facebook.com/country/United%20Kingdom/2013-H2/

[16] Facebook, *Global Government Requests Report*: July 2014-December 2014: https://govtrequests.facebook.com/country/United%20Kingdom/2014-H2/

Transparency of the Use of Communications Data

The reports' findings show disparity between police forces on how many requests are internally rejected/approved. If police forces persist with calls for greater access to our communications, procedures will need to be standardised, transparency about the process published and independent judicial approval brought in as part of the authorisation procedure to ensure that requests for Communications Data are always necessary and proportionate.

Big Brother Watch has previously criticised the lack of information available to the public about how surveillance is conducted. In our 2014 report ***Off the Record*** it was noted that all police forces failed to comply with two thirds of the request; refusing to release information about the use of covert human intelligence and intrusive surveillance.

US based technology companies currently publish far more information on the use of surveillance powers in the UK than the agencies who use them. This makes it difficult to properly assess the scale of use of effectiveness of use of Communications Data. Without this information it is impossible to begin a sensible or informed debate.

It is anticipated that legislation relating to the now severely outdated Regulation of Investigatory Powers Act 2000 and forms of surveillance including Communications Data will feature prominently during the early days of this Parliament. Even if this does not happen, with DRIPA's sunset clause timed for December 2016, a debate will occur.

For there to be a considered debate, accurate evidence such as that provided in this report will be key in framing any argument for or against surveillance legislation.

In 2012 under Freedom of Information law we asked police forces for information about how they use Communications Data. Humberside Police were the only force which were able to provide a breakdown of the offence categories it had used Communications Data for:

---

[17] Daily Mail, *Police struggling to cope with soaring number of child abuse images circulating online warns NSPCC*, 3rd October 2014: http://www.dailymail.co.uk/news/article-2779459/Police-struggling-soaring-number-child-abuse-images-online-warns-NSPCC.html

	Communications Data Requested under RIPA				Requests rejected internally			
	2009/10	2010/11	2011/12	Total	2009/10	2010/11	2011/12	Total
Humberside Police	2,007	1,811	2,316	**6,134**	129	110	102	**341**

Humberside Police Communications Data Breakdown				
	2009/10	2010/11	2011/12	Total
Assault	51	43	96	190
Auto Crime	10	8	20	38
Burglary	121	118	223	462
Criminal Damage	7	15	25	47
Drugs	544	445	371	1360
Missing Persons	100	49	84	233
Murder	196	165	183	544
Organised Immigration Crime	28	56	43	127
Other Crime	340	385	458	1183
Other Non-Crime	64	35	98	197
Rape	24	36	26	86
Robbery	99	98	195	392
Sex Offences	227	198	201	626
Theft	125	90	239	454
Traffic Offences	71	70	54	195

Recent Communications Data Developments

The Intelligence and Security Committee's 2015 report, recommended new categories of information relating to a communication be created.

The Committee found the current definitions to be unclear, due to the potential for information to be described as content as well as communications data. The report put forward a solution; the creation of a '*Communications Data Plus*' and '*Content Derived Information*'. These new categories would "*go further than the who, when and where*".

Communications Data Plus would include information such as:

- The web domains visited by a user.
- The location of the individual(s) involved.

The new category of Content Derived Information would include information that could be obtained through analysing the content of a communication but is still separated from the content itself. This means information such as the accent of a caller would fall into the category.

By adding the two new categories it would become easier to understand the increasing level of intrusiveness that is posed by accessing the following types of information. The safeguards for each would also be more easily applicable:

- Communications Data – Existing safeguards under RIPA.
- Communications Data Plus – "*greater safeguards*" required.
- Content- Derived Information – The safeguards already applied to content would be applied.
- Content – Existing safeguards under RIPA.[18]

As well as the Committee's report, two further reviews are set for imminent publication.

- The Independent Reviewer of Terrorism Legislation, David Anderson QC's, review of investigatory powers and
- The Royal United Services Institute's independent surveillance review.

All three of these reviews will help shape the debate around how law enforcement and intelligence agencies use their powers and how transparent they should be.

[18] Intelligence and Security Committee, Privacy and Security: A modern and transparent legal framework, 12th March 2015, p. 53: https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20150312_ISC_P%2BS%2BRpt%28web%29.pdf?attachauth=ANoY7cqLKesyC8EvkWtAIyEeM1P6Caya1Eg9Y31l4fVTE9MUrtDF6ioZe1_97BbSeXKcTnR-X_c2J6zjKXEBXlf_zB2co_wjJ8nUmGldw5hrhl61tZKhhf7kXFvAkwcdckE_GrGda35osPgM4s_0KVCAB92gulMu_HaUJ8_EOJgyvZagJjy8J3Go0mCexYZL_aL0Z_FlodlWXqAt38can2ANyIYPRCmCobImx7l8OWpzihAx133h9lDjcOMTI6VND1WXx2RzexR2&attredirects=0

Table 4: Requests, Rejections and Approvals Police Forces

Police Force	Communications Data Requested under RIPA				Requests Rejected Internally				Total Approved
	2012	2013	2014	Total	2012	2013	2014	Total	
Avon and Somerset Constabulary	6,561	6,852	5,510	**18,923**	346	330	228	**904**	**18,019**
Bedfordshire Police[19]	1,437	1837	1,895	**5,169**	27	49	49	**125**	**5,044**
British Transport Police	1,070	1,251	1,218	**3,539**	8	7	1	**16**	**3,523**
Cambridgeshire Constabulary	681	909	795	**2,385**	27	50	37	**114**	**2,271**
Cheshire Constabulary[20]	1,691	1,822	2,335	**5,848**	3	2	2	**7**	**5,841**
City of London Police	3,541	4,468	5,501	**13,510**	76	102	90	**268**	**13,242**
Cleveland Police	1,438	1,493	1,345	**4,276**	4	3	7	**14**	**4,262**
Cumbria Constabulary	3,098	3,077	3,630	**9,805**	33	11	30	**74**	**9,731**
Derbyshire Constabulary	1,137	1,681	1,588	**4,406**	68	144	60	**272**	**4,134**
Devon and Cornwall Police[21]	7,361	7,142	5228	**19,731**	128	148	121	**397**	**19,334**

[19] Number returned with advice by SPOC or AO: 2012 - 474, 2013 - 411, 2014 - 922.

[20] The response notes that these figures refer to "*work flow packages*". It adds that "*Each work flow package can contain anything up to 40 separate requests*".

Dorset Police	1928	2828	2831	**7,587**	4	45	68	**117**	**7,470**
Durham Constabulary	1196	1016	4600	**6,812**	6	19	16	**41**	**6,771**
Dyfed Powys Police	1110	900	1149	**3,159**	48	39	33	**120**	**3,039**
Essex Police	5700	7234	6607	**19,541**	1655	1971	1934	**5560**	**13,981**
Gloucestershire Constabulary	869	1338	1295	**3,502**	45	49	29	**123**	**3,379**
Greater Manchester Police		19,037			744			N/A	**18,293**[22]
Gwent Police	1,826	4,616	6,007	**12,449**	47	60	12	**119**	**12,330**
Hampshire Constabulary		**11,750**[23]				**259**			**11,750**
Hertfordshire Constabulary	4,034	5,036	4,844	**13,914**	29	12	17	**58**	**13,856**
Humberside Police	2,942	2,407	3,020	**8,369**	134	127	84	**345**[24]	**8024**
Kent Police	5,099	5,389	5,078	**15,566**	1,279	1,165	1,271	**3,715**	**11,851**
Lancashire Constabulary	4,316	4,810	4,499	**13,625**	53	225	72	**350**	**13275**
Leicestershire Police	3217	3437	2784	**9438**	27	26	34	**87**	**9,351**
Lincolnshire Police		**2,418**				**77**			**2,341**
Merseyside Police	4,543	4,312	3,891	**12,746**	266	212	253	**731**	**12,015**

[21] Response notes that due to a change in working practices within the force applicants can now put multiple requests on one application whereas previously a subscriber application would have to be submitted separately before further applications were submitted. The response therefore continues that in 2014 the 5228 authorisations "*resulted in 10,055 requests*".

[22] The response notes that the figures don't include the number that could have been re-submitted and subsequently approved.

[23] Response notes: "*These figures are based on applications authorised rather than applications originally submitted as some these may have been returned for rework by the applicant and never resubmitted*".

[24] Response notes: "*Our level or rejections can in part be due to administrative error where the applicant launched an incorrect application type. In March 2014 due to modification of the software this significantly reduced the rejections but still launch the incorrect application*".

Metropolitan Police Service	57,710	59,946	59,631	**177,287**	8,861	12,141	11,877	**32,879**	**144,408**
Norfolk Constabulary	2,143	2,036	2,414	**6,593**	67	37	41	**145**	**6,448**
North Wales Police	1,424	1,103	1,228	**3,755**	19	26	6	**51**	**3,704**
North Yorkshire Police	1,096	1211	1302	**3,609**	176	136	184	**496**	**3,113**
Northamptonshire Police	863	1,038	1473	**3,374**	30	56	62	**148**	**3,226**
Northumbria Police	7,649	6,817	6,879	**21,345**	24	20	10	**54**	**21,291**
Nottinghamshire Police[25]	2,546	2,872	4,071	**9,489**	39	31	58	**128**	**9,361**
Police Scotland[26]	18,382	19,390	24,303	**62,075**[27]	451	347	282	**1,080**	**62,075**
Police Service of Northern Ireland	4,939	5,543	4,684	**15,166**	401	484	194	**1,079**	**14,087**
South Wales Police	963	727	1111	**2801**	5	10	9	**24**	**2777**
South Yorkshire Police[28]	Information withheld	6,801	Information withheld	**6,801**		See footnote[29]			
Staffordshire Police	6,039	5,272	5,162	**16,473**	78	183	72	**333**	**16,140**
Suffolk Constabulary	Joint response with Norfolk Constabulary due to "*ongoing collaboration*"								
Surrey Police	**2,828**					**86**			**2,742**

[25] Figures relating to 2012 and 2013 were provided through a previous FOI response, dated 13th November 2014.

[26] Formed in April 2013 - previous figures were provided as totals of the now defunct forces.

[27] This figure represents the total "*numbers of authorisations and notices approved, not applications (or requests). There can be a number of authorisations that emanate from one application*."

[28] A previous FOI request revealed the lines of data requested for each year: 2011-2012: 8921, 2012-2013: 7184 and 2013-2014: 8770.

[29] A previous FOI request provided the following figures for rejections by an approving officer: 2011-2012: 237, 2012-2013: 33 and 2013-2014: 8.

Sussex Police				Did not respond					
Thames Valley Police[30]	6,567	5,897	5,098	**17,562**	180	144	104	**428**	**17,134**
Warwickshire Police	973	834	See West Mercia Constabulary's response.	**1,807**	3	1	See West Mercia Constabulary's response.	**4**	**1,803**
West Mercia Police	3,617	3,533	4,083[31]	**11,233**	20	13	55	**88**	**11,145**
West Midlands Police	31,065	31,074	37,305	**99,444**[32]	323	443	583	**1,349**	**98,095**
West Yorkshire Police	6,807	6,712	6,238	**19,757**	274	280	261	**815**	**18,942**
Wiltshire Police	1317	1614	1402	**4,333**	46	40	12	**98**	**4,235**
Total	**219,487**	**229,474**	**246,329**	**733,237**	**15307**	**19188**	**18261**	**54,164**	**679,073**
Grand Total			**733,237**				**54,164**		**679,073**

[30] Response included the following figures for “data acquisitions”: 2012 - 7531, 2013 - 5897, 2014 – 6661.
[31] 2014 figures - Joint with Warwickshire Police: Part of the "*West Mercia Police and Warwickshire Police Alliance*".
[32] Total refers to the “*Total number of Notices and Authorisations to acquire communications data under Part I Chapter II of the Regulation of Investigatory Powers Act (RIPA).*”

Appendix 1: Methodology

A Freedom of Information request was sent to all local authorities beginning on the 30th January 2015.

We asked for the number of times each force had requested access to communications data as well as the number of occasions a request had been refused.

We received a **92%** response rate. For the purposes of this report responses were included until 22nd May 2015.

Appendix 2: Original Freedom of Information Request

Dear Sir or Madam

I am writing under the Freedom of Information Act 2000 to request information relating to your Force's acquisition of communications data under the Regulation of Investigatory Powers 2000, specifically I am requesting;

1. The number of times your force has requested communications data under the Regulation of Investigatory Powers Act 2000.
2. The number times a request was rejected internally.

I request that the time period covered is 1st January 2012- 1st January 2015.

I further request that the information be broken down by either calendar year or financial year, whichever is most easily accessible to you.

I understand under the Freedom of Information Act that I am entitled to a response within twenty working days. I would be grateful if you could confirm this request in writing as soon as possible.

About Big Brother Watch

Big Brother Watch was set up to challenge policies that threaten our privacy, freedoms and our civil liberties, and to expose the true scale of the surveillance state.

Founded in 2009, we have produced unique research exposing the erosion of civil liberties in the UK, looking at the dramatic expansion of surveillance powers, the growth of the database state and the misuse of personal information.

We campaign to give individuals more control over their personal data, and hold to account those who fail to respect our privacy, whether private companies, government departments or local authorities.

Protecting individual privacy and defending civil liberties, Big Brother Watch is a campaign group for the digital age.

If you are a journalist and you would like to contact Big Brother Watch, including outside office hours, please call +44 (0) 7505 448925 (24hrs). You can also email: info@bigbrotherwatch.org.uk

For written enquiries:

Big Brother Watch

55 Tufton Street

London

SW1P 3QL

www.bigbrotherwatch.org.uk