



Public Bill Committee Chairs  
House of Commons

26 April 2016

## INVESTIGATORY POWERS BILL: PUBLIC BILL COMMITTEE

As promised, I am writing to provide further information on a number of points raised during the course of Committee proceedings on 19 April; the provision of which should allow further informed consideration. I would again like to thank the Public Bill Committee for its continued diligent scrutiny of the Investigatory Powers Bill.

### *Public authorities and authorising officer levels*

There was discussion about the test that public authorities had to meet to justify inclusion in Schedule 4 to the Bill as a public authority that can acquire communications data. Firstly I should say that the public authorities listed in Schedule 4 are, with very limited exceptions<sup>1</sup>, those which Parliament has in the past agreed should have these powers under the Regulation of Investigatory Powers Act 2000 (RIPA). This Bill puts those public authorities on the face of the primary legislation for the first time. For inclusion in the Schedule, each public authority was required to demonstrate:

- i) a continuing need to acquire communications data in order to fulfil their statutory obligations – in the vast majority of cases relating to the prevention and detection of crime; and
- ii) the utility of the communications data which they had acquired under the existing regime in RIPA. This was best demonstrated by the provision of case studies.

I attach a table showing the important work which these public authorities do and the use to which communications data is put. As the Solicitor General noted during the

<sup>1</sup>This Bill provides the Ministry of Defence with the ability to acquire communications data. This corrects an inconsistency in which they were able to intercept communications under the Regulation of Investigatory Powers Act 2000 but not acquire communications data. The Bill also adds the Food Standards Agency (FSA) and Food Standards Scotland to the list of relevant public authorities. The FSA were removed in 2014 but are included in this Bill because of the recent establishment of a national food crime unit within the FSA. The Bill removes powers from the Prudential Regulation Authority.



debate on 19 April, David Anderson QC said in his report "A Question of Trust" that "it should not be assumed that the public interest is served by reducing the number of bodies with such powers, unless there are bodies which have no use for them".

Authorising officer levels reflect the necessary degree of seniority for the person in each public authority to be able effectively to make the considerations required by this legislation. By means of example, there was reference to the rank of the authorising officer in a fire and rescue authority as Watch Manager (Control). This is a senior officer in a fire and rescue authority, who will be experienced and skilled in an often highly pressurised environment, and is best placed to decide when it is necessary to obtain communications data in often life threatening circumstances. None of the levels of authorising officers in public authorities has been reduced from those that currently exist.

It should not be assumed that raising the authorisation level in an authority (which will have been agreed following consultation with the authority concerned) will act as an increased safeguard. Increasing the authorisation levels may lead to requests being authorised by people with a lesser understanding of how communications data is used in operations, understanding that can be key in assessing the necessity and proportionality of any application. Importantly, some of the ranks reflect specific operational requirements of the agencies concerned. It would not be appropriate to raise the authorisation level in a Fire and Rescue body to, say, the Chief Fire Officer, who is not likely to be on duty - and therefore available to approve requests - when a fire breaks out in the early hours of the morning.

#### *Communications data access for local authorities*

During the debate the nature of the test a relevant judicial authority will apply under clause 66(5) in order to approve an authorisation granted by a designated senior officer in a local authority was queried. It is important to look at this provision within the wider context of the authorisation process set out in Part 3 of the Bill.

Any application for communications data made by a local authority is subject to the same stringent restrictions applied to all applications – the important necessity and proportionality considerations, the Single Point of Contact 'guardian and gatekeeper' role and the independent designated senior officer – but with the additional restriction of only being able to be acquired for the statutory purpose of preventing and detecting crime.

We have introduced further safeguards under the Bill in respect of the use of communications data by local authorities. The provisions of clauses 65 and 66 require local authorities to be party to a collaboration agreement under which they must utilise the services of a Single Point of Contact at an independent body – the National Anti-fraud Network – and also require judicial approval for all authorisations. Local authorities will not be able to require internet connection records.

It is within this context of stringent safeguards that clause 66 provides for the additional judicial approval of such applications in order to ensure that any remaining



concerns regarding the acquisition of communications data by local authorities are addressed. The test outlined in clause 66(5) provides for the relevant judicial authority to be reassured that an authorisation has been lawfully granted, as is the case for equivalent approval provisions within Part 3 with which it is aligned; as such, I consider the construct of the test to be appropriate.

#### *Clause 74 – transfer and agency arrangements relating to the filtering arrangements*

I agreed to clarify the effect of clause 74, which provides that the Secretary of State may by regulations transfer any function exercisable in relation to the request filter to a public authority. The intention of this provision is to provide the flexibility required should it be determined that in the future it is no longer appropriate for the Home Office to administer and maintain the request filter.

Schedule 5, amongst other things, ensures that accountability for the request filter will continue to rest with the Secretary of State should its maintenance and operation be transferred to a public authority. Schedule 5 requires the Secretary of State to agree the arrangements made by the public authority for maintaining and operating the request filter. In addition, the public authority must report annually about the functioning of the request filter to both the Secretary of State and the Investigatory Powers Commissioner.

Precisely the same safeguards apply to the request filter whether it is maintained and operated by the Secretary of State or a public authority. This includes oversight of its operation by the Investigatory Powers Commissioner; that it may only be used in response to a properly authorised request for communications; and that any data obtained by the request filter in pursuance of an authorisation is immediately destroyed when the purpose of the authorisation has been met.

#### *Enforcement of extra-territorial jurisdiction*

During the debate on Part 3 the issue of extra-territorial jurisdiction was raised. Terrorists and criminals use a range of diverse communications services, many of which are provided by overseas companies. For that reason, UK law has long been clear that those providing communications services to users in the UK have an obligation to comply with UK warrants requesting the content of criminals' and terrorists' communications and with notices requiring the disclosure of communications data. The Investigatory Powers Bill maintains that position. It does not extend extra-territorial jurisdiction. A company only has to comply with a warrant or request where it is reasonably practicable for it to do so, including considering whether doing so could be in conflict with the domestic laws of the jurisdiction where they are based.

There are seven powers in the Bill which provide for a communication service provider to be required to assist and provide or retain data. The Bill makes clear that all seven of these requests can be made to an overseas provider, but the duty to



comply can only be enforced in respect of those three powers (targeted and bulk interception, and targeted requests for communications data) that can be enforced against an overseas provider under existing legislation. Where a duty can be enforced against an overseas provider, the Bill makes clear that the laws of the jurisdiction in which it is based must be taken into account to consider whether the action required might lead to a breach of those local laws. All requests for assistance can be made to anyone providing services to the UK, irrespective of where they are in the world – but it is critical that interception warrants and targeted communications data request can be enforced. Operations to protect the public from terrorism and solve crimes in many cases currently rely on these powers. We are not looking to expand our powers in relation to extra-territorial jurisdiction in respect of any other powers in the Bill.

### *Internet connection record definitions*

There were a number of questions concerning which part of the definition of an internet connection record specifically prevents a full URL from forming part of an internet connection record. I would like to clarify this issue.

The definition of an internet connection record in clause 54(6) of the Bill sets out the subset of communications data that constitutes an internet connection record. Communications data is then defined at clause 223(5) of the Bill. In particular, 223(5)(a)(ii) states that events data is data that:

*is comprised in, included as part of, attached to or logically associated with a communication (whether by the sender or otherwise) for the purposes of a telecommunication system by means of which the communication is being or may be transmitted.*

In short, this means that for an internet connection record to meet the definition of communications data it must be data that is necessary for the communication to be delivered to its destination. When browsing the internet, a URL serves two main purposes. Firstly, some elements of a URL operate to deliver a communication to its intended destination. This will be another computer or server connected to the internet. Data that is needed for this would meet the definition of communications data. Secondly, the remaining elements of the URL tell the server how to respond; for example, to request specific content from the server. Because these elements are not needed to deliver the communication, they are not communications data.

An example would be [www.bbc.co.uk/politics/story](http://www.bbc.co.uk/politics/story). In this example [www.bbc.co.uk](http://www.bbc.co.uk) would route a communication to the BBC server and would therefore be communications data. The segment of the URL that includes 'politics/story' would tell the server which story to send back and would not be communications data. As such, the full URL [www.bbc.co.uk/politics/story](http://www.bbc.co.uk/politics/story) could not be retained or accessed under the communications data powers in the Bill, and all that would be retained would be [www.bbc.co.uk](http://www.bbc.co.uk). Importantly, because telecommunications operators need to route the communication, they are able to determine the data that meets the relevant definition on their network.



### *Retention of third-party data*

As the Home Secretary explained during the debate at Second Reading and I reiterated during the Committee debate on Part 4, we will not require the retention of third party data. We consider the Code of Practice the best place to make that policy clear. However we are prepared to consider whether there are other possibilities that do not inadvertently prohibit the legitimate retention of data that operators use or store for their business purposes.

### *Data security*

During the debate on Part 4 of the Bill there were a number of questions concerning data security, in particular relating to offences that exist concerning the theft of data. In my letter of Tuesday 19 April, I provided a table covering a number of relevant offences. For example, the table explained that sections 55(1), 55(4) and 55(5) of the Data Protection Act 1998 provide for various offences, including an offence of knowingly or recklessly obtaining, disclosing or procuring personal information without the consent of the data controller; and selling or offering to sell such personal data.

Should any data retained by telecommunications operators under Part 4 of the Bill be acquired, stolen or sold, one of these offences is likely to have been committed. However, it is of course important to ensure that robust security requirements are in place that can help prevent retained communications data being stolen in the first instance. As I explained, telecommunications operators have to comply with the Data Protection Act 1998 and the Privacy and Electronic Communication Regulations 2003, which both include requirements to ensure appropriate security of personal data. On top of those general requirements, telecommunications operators subject to data retention notices will have to comply with the security requirements in clause 81 and the more detailed security requirements in the draft Communications Data Code of Practice, as well as any specific requirements in the retention notices themselves.

Furthermore, clause 210 requires the Information Commissioner to audit compliance with security requirements. This aligns with the Information Commissioner's other responsibilities in respect of data security. For example, the Commissioner is responsible for investigating the Data Protection Act offences outlined above.

### *Communications obtained by equipment interference warrants*

I committed to provide clarification on what communications may be obtained through equipment interference warrants. Clause 3(4) makes clear that the offence of unlawful interception applies to communications in the course of their transmission and communications stored on the system.

Like RIPA, the Bill also lists the ways in which lawful authority can be given to intercept communications (clause 5). Clause 5(1)(c) allows stored communications to be obtained by other statutory powers, including equipment interference warrants.



So, clause 88(6) simply reiterates the effect of clause 5 (and clause 2), so that interception of communications in the course of their transmission is an offence unless authorised in one of the ways set out in clause 5.

'Live' communications can be authorised in the ways set out in clause 5(1)(a) or (b) (which does not include equipment interference warrants).

Stored communications, however, can be intercepted either:

- in accordance with clause 5(1)(a) or (b)); OR
- alternatively, in accordance with clause 5(1)(c), using an equipment interference warrant (or other statutory power such as the Police and Criminal Evidence Act 1984).

Clause 88(6) therefore simply makes explicit that an equipment interference warrant cannot authorise interception other than the interception of stored communications. This is necessary to ensure that, for example, when an equipment interference warrant is issued in order to obtain the information stored on a hard drive or a smartphone, the warrant can authorise the examination of material on the device including stored communications. The clause further ensures that equipment interference warrants cannot be used to authorise interception in 'real time'. This is, in effect, the same position as under RIPA.

### *Equipment data*

I committed to write further in relation to the definition of equipment data in clause 89. This concerns the issue of 'inferred meaning' which is an important principle that applies across the Bill. Clause 223 of the Bill defines both communications data and content. While the Committee will turn its attention to this clause in due course I think it is helpful for me to refer to it now as it is perhaps easier to explain the principle in this context.

The definition of the content of a communication specifically excludes meaning arising from the fact of the communication or data relating to its transmission. It may be possible to infer meaning from almost any action or piece of data – for example, it could be inferred that two people know one another based on the fact, and frequency, of their communications. These inferences may not always be accurate or reliable – these people may not actually know each other.

The key point of the inferred meaning exclusion is to make clear that although it is possible to infer some meaning from the fact a communication has taken place, that meaning does not form part of the content of the communication.

Clause 89 applies that same principle in the context of equipment interference. A device may contain stored communications and other items of information such as documents, spreadsheets or photographs. An investigator may be able to infer something from simply the fact that the data is held by a person on a device but that



meaning does not form part of the content of those stored communications or items of information.

Clause 89 ensures that data is treated consistently across the Bill so that in the context of equipment interference, the content of communications and items of information on a device is subject to higher safeguards than the simple fact of those communications or the existence of the items of information.

### *Thematic warrants*

We discussed the issue of thematic warrants during the debate, in particular the need for equipment interference warrants that might relate to more than one person where a crime or terrorist act is being perpetrated by multiple actors.

There is one point that I would like to follow up on in this letter. There was a reference to David Anderson's comments about the breadth of the equipment interference warrants provided for in the Bill. I would like to be clear that these provisions are strictly limited. The double-lock authorisation process will ensure that warrants can only be issued where necessary and proportionate. The Investigatory Powers Commissioner in overseeing all of these powers will ensure that the breadth of warrants issued under this Part will be appropriate. I would also like to direct the Committee to page 26 of the draft Equipment Interference Code of Practice, which requires that warrant applicants be as specific as possible when describing the subjects of any proposed interference: "A targeted warrant must sufficiently define the equipment to which it relates, whether by reference to persons, a group, location etc, so that the extent of the interference to be authorised is reasonably foreseeable". The requirement for the application to have sufficient information for the authorising person to make an assessment of necessity and proportionality is a key point that the Investigatory Powers Tribunal found supported the use of thematic warrants in their judgement earlier this year (IPT 14/85/CH). It has also been reflected, in the context of interception, by the previous Interception of Communications Commissioner's report published in March 2015 (page 36).

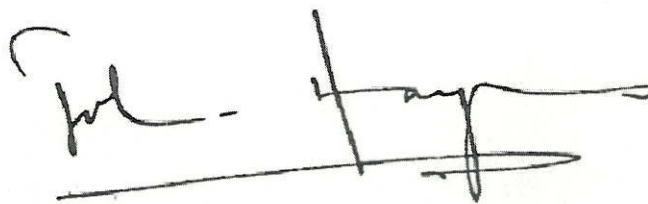
Taken together, these provisions mean that the issuing authority and Judicial Commissioner will receive warrant applications containing as much information as possible, allowing them to make well informed decisions about the breadth of any interference that they authorise. The provisions in clause 90 simply ensure that warrants can be sought on the terms that the equipment interference agencies require.

The Committee touched briefly on bulk equipment interference, and whether such a power is needed given the possible breadth of warrants in the targeted regime. This was a point also raised by the Intelligence and Security Committee of Parliament (ISC) as part of its report on the draft Bill. The difference between the two regimes is not a rigid definition based on the scale of the interference. Rather, the bulk equipment interference regime is tailored to provide additional safeguards for operations that seek to acquire information that may need further sifting before the key items of information are identified. This is akin to the longstanding bulk

interception regime both in terms of the process of sifting data and the safeguards applied to the material.

I am pleased that following further discussions with the ISC they are now satisfied of the requirement for the two separate regimes, as Dominic Grieve confirmed during Second Reading of the Bill.

I hope this provides the Public Bill Committee with the additional information needed. I am copying this letter to Committee members and the Clerks.

A handwritten signature in black ink, appearing to read 'John Hayes', with a long horizontal line extending from the end of the signature.

**RT HON JOHN HAYES MP**



Schedule 4 to the Investigatory Powers Bill lists the relevant public authorities for the acquisition of communications data. The following table provides a brief explanation for why each of the 'minor users' of communications data are included in the Bill.

The table does not include the police, security and intelligence agencies, Her Majesty's Revenue and Customs, the Home Office (for border and immigration investigations) or the Ministry of Defence.

**Table 1: Reasons relevant public authorities require the ability to acquire communications data**

| Public authority         | Reason the authority requires the ability to acquire communications data   |
|--------------------------|--|
| Department of Health     | <p>The Medicines and Healthcare Products Regulatory Agency is part of the Department of Health and is the principal law enforcement agency with responsibility for investigating criminal acts relating to medical products (medicines and devices). The Agency enforces the provisions of the Human Medicines Regulations 2012, the Medicines Act 1968, the Blood Safety and Quality Regulations 2004, the Good Laboratory Practice Regulations 2005 and the Health Ministers and Medical Devices Regulations 2003.</p> <p>In practice, communications data is used in investigating serious crimes, such as counterfeiting medicines. For example, communications data can demonstrate links between conspirators.</p> <p>In November 2014 the Department of Health also set up an Anti-Fraud Unit. Investigators have powers under the National Health Service Act 2006 to prevent, detect and investigate offences and other unlawful activities carried out against the health service.</p> |
| Ministry of Justice      | <p>The National Offender Management Service acquires communications data in order to investigate allegations regarding crime committed against the Prison Act 1952. Often investigations will be linked to corruption allegations against prison staff or official visitors to the prison.</p> <p>It uses communications data to investigate offences involving staff corruption, in particular the supply of illegal drugs in prisons.</p>  |
| Department for Transport | Accident Investigation Branches use communications data in investigations into accidents,  |



|  |   |
|--|---|
|  | <p>for example if a flight crashes the investigation branches may need to determine if the pilot was using a mobile phone at the time of the crash.</p> <p>The Maritime and Coastguard Agency acquire communications data very rarely but when they do it is likely to be in threat to life situations, for example to locate someone lost at sea.</p>  |
| Department for Work and Pensions                                   | <p>DWP currently uses powers under the Social Security Administration Act 1992 to obtain communications data in order to support its functions of detecting, prosecuting and preventing social security benefit offences. For example, where someone is defrauding the benefit system by pretending they are not living at a certain address, communications data is used to link them to that address.</p> <p>The Child Maintenance Group have responsibility for the calculation and collection of child maintenance. Communications data is used to investigate fraud against the child maintenance system, including bogus second applications to reduce liability, claiming to be outside the jurisdiction of the scheme and conspiracy with others to obtain a negative paternity result. For example, communications data can be used to identify the address of the fraudulent applicant.</p> |
| Competition and Markets Authority                                  | <p>The CMA acquires communications data in the course of investigating breaches of competition law under the Competition Act 1998 and the Enterprise Act 2002. For example, communications data can be essential in demonstrating links between companies that are operating as a cartel.</p>   |
| Criminal Cases Review Commission                                   | <p>The CCRC acquires communications data in respect of investigations into miscarriages of justice. For example, it has used communications data as new evidence, for example to demonstrate communications (and the length of communications) between a complainant and someone who has potentially be wrongfully convicted of an offence.</p>   |
| Department of Enterprise, Trade and Investment in Northern Ireland | <p>DETINI are able to acquire communications data because in Northern Ireland they, rather than local authorities, have responsibility for investigating trading standards offences.</p>  |
| Financial Conduct Authority  | <p>The FCA has civil and criminal powers under the Financial Services and Markets Act 2000 to investigate issues such as insider dealing and</p>  |



|   |  |
|---|--|
|   | market manipulation. In such cases being able to demonstrate communications between suspects is essential.   |
| A fire and rescue authority under the Fire and Rescue Services Act 2004 | The fire and rescue services may need to acquire communications data in an emergency to prevent death or injury. For example, it can be used to identify the location of someone who has contacted the emergency services.   |
| Food Standards Agency   | In January 2015, following a number of independent reviews in response to the horsemeat scandal, the Government established a National Food Crime Unit (NFCU) as part of the Food Standards Agency. Food crime is such that it is important to establish the supply chains, communications data will be used to demonstrate links between each section of the chain. The NFCU investigates serious offences, including under the Fraud Act 2006.                   |
| Gambling Commission   | The Gambling Commission are responsible for prosecuting a number of offences under the Gambling Act 2005. For example, the Commission investigates unlicensed bookmakers who provide illegal gambling services and the illegal supply of gaming machines. Communications data is used to demonstrate links between the suspects and victims, for example where an unlicensed bookmaker is conducting the illegal gambling via telephone.                           |
| Gangmasters Licensing Authority   | The Gangmasters Licensing Authority was established under the Gangmasters (Licensing) Act 2004 following public concern at the lack of action to prevent the deaths of migrant cockle pickers in Morecambe Bay. It issues licences only to approved gangmasters and investigates and prosecutes those without a license. Communications data can link unapproved gangmasters to the migrants they are exploiting, including cases of forced and compulsory labour. |



|   |  |
|---|--|
| Health and Safety Executive                         | The Health and Safety Executive enforces health and safety legislation. It investigates and prosecutes offences which involve the creation of serious risks to people such as explosions from faulty domestic gas installations and major chemical incidents. Communications data can be used to identify perpetrators, for example by placing them at the scene of a faulty installation.   |
| Independent Police Complaints Commission            | The IPCC undertakes independent investigations into the most serious cases of police criminality and misconduct, including deaths and serious injuries and other alleged human rights abuses. For example, if someone dies following contact with a law enforcement agency, the IPCC may acquire communications data to identify the deceased's movements prior to the incident and to identify potential witnesses.   |
| Information Commissioner                            | The Information Commissioner is the independent supervisory authority responsible for enforcing the provisions of the Data Protection Act 1998 and the Freedom of Information Act 2000. The Commissioner's Office uses communications data where necessary to assist in identifying offenders attempting unlawfully to obtain, disclose, sell or offer to sell personal data in contravention of the above legislation.  |
| National Health Service Business Services Authority | The NHS Counter Fraud and Security Management Service is the body charged with tackling crime within the NHS, including having responsibility for leading investigations into serious, organised and/or complex financial irregularities and losses which give rise to suspicions of fraud, bribery or corruption. Communications data is used to demonstrate links between conspirators, for example those involved in the production of fraudulent invoices for substantial sums of money. |
| Ambulance services                                  | The ambulance services may need to acquire communications data in an emergency to prevent death or injury. For example, it can be used to identify the location of someone who has contacted the emergency services.   |

|                      |  |
|----------------------|--|
| Ofcom                | Ofcom is the independent regulator and competition authority for all the UK communications industries, with responsibilities across television, radio, telecommunications and wireless communications services. It acquires communications data to investigate the location and operation of illegal radio broadcasters under the Wireless Telegraphy Act 2006. It also has responsibility to investigate certain offences, such as cartel offences involving communications services, under the Competition Act 1998. |
| Serious Fraud Office | Under the Criminal Justice Act 1987, the Serious Fraud Office investigates, prosecutes, and deals with asset recovery in respect of the topmost tier of serious or complex fraud, including bribery and corruption. Communications data can demonstrate links between the suspects to prove the substantive offence, and any conspiracy or joint enterprise.   |

### Local authorities

Local authorities are not included in Schedule 4 because they are covered by specific provisions elsewhere in the draft Bill. This is because they must go through a system of enhanced safeguards before being able to acquire communications data. Including the requirement to make their requests for communications data through the Single Points of Contact at the National Anti-Fraud Network and magistrate approval. Local authorities are responsible for investigating a range of serious offences, including under the Trade Marks Act 1994 and the Fraud Act 2006, such as scams to target the elderly, rogue traders, environmental offences such as dumping hazardous waste illegally and benefit fraud.