BIG BROTHER WATCH
DEFENDING CIVIL LIBERTIES, PROTECTING PRIVACY

Investigatory Powers Bill Briefing

What is the Investigatory Powers Bill?

Running to 245 pages, the Investigatory Powers Bill is an attempt to establish a clear framework for the authorisation and use of surveillance powers available to our law enforcement and intelligence agencies.

The Bill avows many of the existing surveillance powers available to the intelligence agencies, but it also expands some of their uses to the police and creates additional surveillance powers, including Internet Connection Records (ICRs) and a Request Filter process.

The avowed powers include:

- **Equipment Interference** - better known as the hacking of computers, phones and other commonplace, every day connected devices.
- **Data retention** – the storage and access of communications data for 12 months as legislated for in the Data Retention and Investigatory Powers Act (DRIPA)
- **Interception** – the bulk and targeted surveillance of communications, telephone calls and internet activity.
- **National Security Notices and Technical Capability Notices** - the requirement for private companies to build systems to retain data and provide information on customers/users on demand.

The creation of **Internet Connection Records** which will require the communications service providers to hold data about the websites we visit and devices we use for 12 months. A **Request Filter** will be built to act as a data centre go-between for public authorities requesting data from the telecommunications companies.

The Bill also proposes a new **authorisation process** for warrants, defined as a **"double lock"** of both Ministerial and Judicial approval.

Timetable of the Bill

A draft of the Bill was published for pre-legislative scrutiny on 4th November 2015.

Three Parliamentary committees scrutinised its proposals.

1. **The Joint Committee on the draft Investigatory Powers Bill** established specifically to look at the draft Bill as a whole
2. **The Science and Technology Committee** looked at the technical capabilities in the draft Bill.
3. **The Intelligence and Security Committee** looked specifically at the work of the intelligence agencies.

Despite the very limited time available to scrutinise the hefty draft Bill all three committees published their reports at the beginning of February.

They roundly criticised the draft Bill, with serious concern expressed about the lack of clarity, lack of evidence, lack of privacy and the lack of clear operational purpose for the powers.

In total 123 recommendations were made by the three committees, many of which have not been adopted by the Home Office.

Despite such marked concerns, the Home Office published the Bill a mere three weeks after the final committee's report was published, accompanied by almost 600 pages of supplementary draft Codes of Practice, operational cases and response documents.

DRIPA Sunset Clause

One element of the Bill; the part which will replace the Data Retention and Investigatory Powers Act 2014 (DRIPA), is subject to a sunset clause; currently set to expire at the end of this year.

This element of the Bill which deals with the retention of data for 12 months could be split and dealt with accordingly, leaving the rest of the Bill to be given proper, full Parliamentary consideration.

However the Home Office seem stubbornly set on their current course to keep the Bill combined and proceed with seeking Royal Assent for all powers, new, old and those not subject to the sunset clause.

This leaves parliament working to a timetable, which although not expedited, is rushed, and leaves little time for detailed examination of the 900 pages of documents associated with the Bill, pages which should be read to ensure the most basic understanding of the powers contained, some of which do not appear in detail on the face of the Bill.

The Bill will be given its **Second Reading on Tuesday 15th March**.

This Briefing

This briefing explains the key concerns about the Bill and suggest ways you might wish to engage with the debate to ensure that the law is the best it can possibly be and that powers which you legislate for are the very best at protecting the country's freedom and security.

Alongside this briefing we have provided a number of factsheets which detail in simple terms the key parts of the Bill. We also recommend that you read the House of Commons Library Briefing Paper Number 7518 which offers an excellent breakdown of the recommendations made to improve the Bill many of which were not accepted by the Home Office but which remain key areas of improvement.

It is important that the issues in the Bill are given the consideration they deserve. Surveillance powers are a critical element to maintaining the security of the country, this must be dealt with accordingly and be subject to a proper, informed debate.

BIG BROTHER WATCH
DEFENDING CIVIL LIBERTIES, PROTECTING PRIVACY

Key Areas of Concern

Data Retention

1. Retention Notices, National Security Notices and Technical Capability Notices should all be subject to authorisation by the Secretary of State and a Judicial Commissioner
2. Telecommunications Services should not be required to remove encryption.
3. Internet Connection Records should be removed from the Bill.
4. Greater scrutiny of the plans for a state operated Request Filter.

Targeted Interception

1. Major modifications to a warrant should be authorised by a Judicial Commissioner.
2. Material gained through interception should be used as evidence in court.

Bulk Powers

1. Bulk Equipment interference should be removed from the Bill.
2. Clarity should be provided on what constitutes a Specific Bulk Personal Dataset and confirmation that medical records are not included must be given.
3. Class Bulk Personal Datasets should be removed from the Bill.
4. The role of Judicial Commissioners in relation to Bulk Personal Datasets should be made clear on the face of the Bill.

Equipment Interference

1. The authorisation process for Equipment Interference warrants should be the same for each organisation.
2. Targeted Equipment Interference should be more tightly defined.

Safeguards

1. A real “double lock” system for the authorisation of warrants should be introduced.
2. Judicial Commissioners should be appointed by the Judicial Appointments Committee.
3. Discussions about the staffing, funding and resourcing of the IPC should be open to a broad range of individuals and organisations.
4. Proposals for user notification should be strengthened to create a system that brings real redress.
5. The Bill should be subject to the same review as the National Security Strategy and Strategic Defence Review

BIG BROTHER WATCH
DEFENDING CIVIL LIBERTIES, PROTECTING PRIVACY

Data Retention

Relevant Sections of the Bill

Part 3: Authorisation for obtaining communications data.
Part 4: Retention of communications data.
Part 9: Chapter 1: Miscellaneous and General Provisions

Our recommendations

1. Retention Notices, National Security Notices and Technical Capability Notices should all be subject to authorisation by the Secretary of State and a Judicial Commissioner.
2. Telecommunications Services should not be required to remove encryption.
3. Internet Connection Records should be removed from the Bill.
4. Greater scrutiny of the plans for a state operated Request Filter.

What is communications data?

Communications Data is a key element of the Bill, yet the definitions given in **Part 9, Chapter 2, Section 223** remain extremely complicated; to the extent that they rarely, if ever, provide complete clarity. Without clarity how can any of us fully understand what is being legislated? In an attempt to explain and understand the various definitions and use of communications data we have written a **Communications Data Factsheet which can be found here:**

What does the Bill say and do?

The Bill makes provision for the acquisition, retention and analysis of letters, phone calls, email and other internet or mobile communications by the police, intelligence agencies and other public authorities including HMRC and the NHS. Many of these powers are already in law. Part 1, Chapter 2, Section 21 of The Regulation of Investigatory Powers Act 2000 allows for the acquisition and disclosure of Communications Data**.**
The Investigatory Powers Bill will ensure that **existing powers are made lawful,** including the ongoing retention of all of our communications for 12 months which was made law under emergency legislation in DRIPA before the sunset clause kicks in at the end of the year.

It is worth noting that **DRIPA** and the retention of our communications data for 12 months is currently **being addressed in the Court of Justice in Europe,** in a case brought by David Davis MP and Tom Watson MP who claim that DRIPA is **incompatible with Article 8** of the European Convention on Human Rights; the **right to respect for private and family life** and **Articles 7 and 8** of the EU Charter of Fundamental Rights, **respect for private and family life and protection of personal data.**

Retention Notices

The Bill will allow a Secretary of State to order telecommunications operators to retain communications data by issuing a **Retention Notice**:

Part 4, Section 78, Clause 1

> *The Secretary of State may by notice (a "retention notice") require a telecommunications operator to retain relevant communications data if the Secretary of State considers that the requirement is necessary and proportionate.*

This section of the Bill will require **all telecommunications operators** to retain all of their users Communications Data for up to 12 months. In the Bill Telecommunications Operator is defined in the Bill as:

> *A person who—*
> *(a) offers or provides a telecommunications service to persons in the United Kingdom, or*
> *(b) controls or provides a telecommunication system which is (wholly or partly)—*
> *(i) in the United Kingdom, or*
> *(ii) controlled from the United Kingdom.*

This is an **incredibly broad definition** which encompasses any person, system or provider of communications, including, any internet service, email, app, cloud provider, wi-fi provider (including public spaces, hotels, cafes, restaurants, pubs, public transport), health devices, cars and so on….

The **detail of** what will be required by a Telecommunications Operator is **not outlined on the face of the Bill** but in the draft code of practice.

It includes the requirement for a company to *"take such steps as are necessary to ensure that data which is generated and processed by the CSP (Communications Service Provider) but not collected for business purposes is made available to be retained."* It goes on to require that the data is processed to *"ensure that multiple items of data" are "stored in a single clear record".*

We are led to believe that these requirements as well as many others in the Bill are over and above the current capabilities of some CSPs. This could be perceived as one of the key problems highlighted by **the Science and Technology Committee** who raised concern that the Bill may place UK businesses at a *"commercial disadvantage compared with their overseas competitors."*

The retained data will be available to law enforcement agencies, intelligence agencies, local authorities as well as some government departments, to access under a warrant signed off internally by a "*designated senior officer*". **Part 1 of Schedule 4** lists who within each organisation can sign off a warrant.

No Telecommunications Service will be permitted to disclose the fact that they have been served with a retention notice.

National Security Notice and Technical Capability Notice

Companies will be required to retain data on order of either a **National Security Notice**:

Part 9, Chapter 1, Section 216

> *The Secretary of State may give any telecommunications operator in the United Kingdom a notice (a "national security notice") requiring the operator to take such specified steps as the Secretary of State considers necessary in the interests of national security.*

Or a **Technical Capability Notice**:

Part 9, Chapter 1, Section 217

> *The Secretary of State may give a relevant operator a notice (a "technical capability notice")*

And....

> *The obligations that may be specified in regulations under this section include, among other things –*
>
> *(a) obligations to provide facilities or services of a specified description;*
> *(b) obligations relating to apparatus owned or operated by a relevant operator;*
> *(c) obligations relating to the removal by a relevant operator of electronic protection applied by or on behalf of that operator to any communications or data.*

Part 8 of the Interception of Communications draft Code of Practice accompanying the Bill outlines in more detail that only companies of 10,000 users or more will have to adhere to a notice but smaller companies may have to oblige a warrant. It also states that obligations of a notice will include **removing encryption**, providing facilities and services of a specific description, obligations relating to apparatus owned by the company.

Request Filter

The Bill calls for a **Request Filter** to be created, to act as a go-between for the public authorities who request access to communications data and the Telecommunication Services who hold it.

This **Request Filter** is outlined in **Part 3, Section 58** of the Bill**.**

The **real detail** of the capability is outlined **not in the Bill** but in **Section 9 of the draft Communications Data Code of Practice** which states that

"The request filter will be operated on behalf of the Secretary of State by the Home Office. In practice the service will be provided by one or more third parties under contract" and that *"the data processor for all data disclosed to the request filter will be the Home Office (or another public authority designated by the Secretary of State by regulations.)"*

In summary the Filter will have the power to **obtain** the data from the telecommunications services, **process** and **retain** the data, and then **disclose** it to the relevant person who has been authorised by a warrant to access and analyse the data further.

Whilst these provisions will enable the retention and subsequent warranted acquisition of communications data, the Bill also proposes the creation of a new form of data to be held, the **Internet Connection Record.**

Internet Connection Records

Internet Connection Records (ICRs) are a detailed log of an individual's browsing history. It is assumed that each ICR will detail the communications data (not the content) of each website a person visits, this means the, date and time of the visit, the length of time spent on a website, the detail of the device used, including the device being connected to and the IP address - which can be used to determine exactly where you are.

Whilst internet connection records feature only four times in the Bill, including a reference to where the definition can be found, some detail can be found in **Part 7 of the Communications Data draft Code of Practice**.

For more information about Internet Connection Records please see our Factsheet here.

What are the problems and what can you do?

1. Retention Notices, National Security Notices and Technical Capability Notices should all be subject to authorisation by the Secretary of State and a Judicial Commissioner.

Only the Secretary of State has the power to authorise a Retention Notice, National Security Notice and Technical Capability Notice. This is not in keeping with the rest of the Bill which requires a Judicial Commissioner to be involved in the "review" and "approval" of many of the most vital and intrusive capabilities.

These notices will in effect enable the Secretary of State to demand private companies act as a facilitator, depository and provider of people's communications. Independent oversight such as authorisation by a Judicial Commissioner, of such powers is critical to maintain necessity, proportionality and transparency.

The only involvement a Commissioner will have is at the point of annual review, and even then the requirement will be for consultation only.

Section 216 on **National Security Notices** avows the power of Section 94 of the Telecommunications Act 1984.

Section 94 was used to monitor the communications of all UK citizens post 9/11. Whilst we would hope the avowal of the capability would provide more transparency and scrutiny of its use, the lack of any independent approval or review of the authorisation, or indeed more preferably

independent authorisation, is of deep and profound concern. Particularly when it is illegal for a Secretary of State to discuss these warrants before Parliament.

It is also critical that Parliament ascertains the detail of what private companies will be required to do to build systems purely to satisfy the requirements of the State.

2. The removal of encryption raises profound technical and moral concern.

Whilst the Home Office are keen to stress that the Bill does not call for the weakening of encryption or the building of "backdoors", it is clear in the draft Code of Practice that companies will be required on receipt of a warrant or a technical capability notice, to **remove encryption when possible**. This requirement has the potential to impact the security of an individual's data.

The removal is, and has been since the dawn of the internet, a very contentious issue. A recent speech by **Robert Hannigan, Director of MI6** at MIT recently outlined many of the problems. He clearly stated that *"The solution is not, of course, that encryption should be weakened, let alone banned."*

He went on to say that despite the Bill calling for Tech Companies to remove encryption when asked, he believes that *"We will need a new forum….bringing together the tech industry, Government agencies, academia and civil society. A space where we can build confidence, have a frank dialogue, and work out how we can best tackle the problems we all recognise within the law."* and that *"Our Prime Minister will be setting out further details in the coming months on how the UK Government plans to facilitate this dialogue on our side of the water."*

It is critically important that encryption be debated properly by both Houses. Many key academics have raised concern about any form of weakening or removal of encryption. If the Prime Minister is intending on encouraging a private group to be formed to discuss how best to navigate the encryption problem, are the recommendations outlined in the Bill and the draft Code of Practice, appropriate to be passed at this stage? **Further informed discussion should be had before legislation is passed.**

3. Internet Connection Records should be removed from the Bill.

Internet Connection Records have been likened by the Home Secretary to *" the modern equivalent of an itemised phone bill"*; this has been roundly acknowledged as inaccurate. A phone bill outlines a one to one connection, whereas an internet connection is a one to many connection.

Our browsing history is considered to be personal information. Even just listing the websites we visit can reveal more about us than we realise, particularly if that data is cross referenced against other data or used for profiling purposes.

Little information has been presented by the Home Office. ICRs still have not been clearly defined in either the Bill or the accompanying draft Code of Practice. During the evidence sessions to the Joint Committee no evidence was presented to clearly outline how they will work, exactly how much they will cost and whether or not they are a) technically feasible or b) beneficial to the purpose which the Home Office believe they are necessary.

Furthermore no information has been published to make the case for why the UK needs them more than anyone else. If the scheme is implemented **the UK will be the only European or Commonwealth country to have such as system.**

Australia recently introduced new data retention laws but they explicitly prohibited the collection of browsing histories[1].

Denmark introduced a similar system in 2007, which was scrapped seven years later because it failed to provide results and had been proven to be of no real use or benefit to law enforcement[2].

The Home Secretary in evidence to the Joint Committee stated that ICRs will differ from the Danish scheme in "*a number of ways*"[3] but despite calls in the Joint Committee report for the Government to *"publish a full assessment of the differences between the ICR proposal and the Danish system alongside the Bill"* this has not been done.

Furthermore **The Science and Technology Committee** raised concern about the "*commercial disadvantage*" that businesses based in the UK might face if required to build systems to store ICRs.

The Intelligence and Security Committee pointed out that "*the Agencies have told told the Committee that they have a range of other capabilities which enable them to obtain equivalent data*." If this is the case, the requirement for new systems to be built and the web browsing of us all on mass to be gathered and stored for a year seems somewhat at odds with the critical concepts surveillance only when of necessary and proportionate.

The lack of precise detail or proof of the benefit of collection of Internet Connection Records and the fact that similar data is being obtained by other means does not justify the proposal becoming law.

We propose that ICRs are removed from the Bill.

---

1 The Parliament of the Commonwealth of Australia, *Telecommunications (Interception and Access) Amendment Act 2015*, 13th April 2015: http://parlinfo.aph.gov.au/parlInfo/download/legislation/bills/r5375_aspassed/toc_pdf/14242b01.pdf;fileType=application%2Fpdf

2 IT-Political Association of Denmark, *Written Evidence to the Joint Investigatory Powers Bill*, Page 1: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/draft-investigatory-powers-bill-committee/draft-investigatory-powers-bill/written/26354.pdf

4. Greater scrutiny of plans for a state operated request filter.

No information has been provided about who will be in charge of building the Request Filter, other than it will be a contract handed to a third party. Given government's poor history when it comes to the commissioning and running of IT projects, the lack of any clarity on this issue is of concern.

As the internet and mobile technology become embedded further into our lives, with the intention of all our devices, cars and homes being connected in the not too distant future, the level of data which will fall into the category of communications data will increase exponentially. Citizens therefore have a right to know that when they engage with a private company their data will not be held in a state approved system for the purpose of potential surveillance.

Parliament should scrutinise and question the Request Filter very carefully, to ensure that a "honeypot" of communications is not being created and that clarity is given over how the Filter will be built, used and maintained.

BIG BROTHER WATCH
DEFENDING CIVIL LIBERTIES, PROTECTING PRIVACY

Modification of interception warrants and use of intercept as evidence

Relevant Sections of the Bill

Part 2: Lawful interception of communications

Our Recommendations

1. Major modifications to a warrant should be authorised by a Judicial Commissioner.
2. Material gained through interception should be used as evidence in court.

What does the Bill say and do?

Warrants are a critical part of the Bill. Part 2, Chapter 1 outlines the process of seeking a warrant for the interception of communications as well as the authorisation, renewal and the modification of a warrant.

Modification of warrants is outlined in **Part 2, Chapter 1, Section 30, Clause 1**

> *The provisions of a warrant issued under this Chapter may be modified at any time by an instrument issued by the person making the modification.*

The Bill goes on to outline the **difference** between a **minor modification** and a **major modification**.

Subsection 30 (2)(a) describes major modifications as:

> *adding, varying or removing the name or description of a person, organisation or set of premises to which the warrant relates*

Altering any other part of a warrant is classed as a **minor modification**.

For more information about warrants please see our Warrant Factsheet here.

The Bill continues to maintain that **intercept as evidence** is not permitted for use in court.

Part 2, Chapter 3, Section 48, Clause 1 states:

> *No evidence may be adduced, question asked, assertion or disclosure made or other thing done in, for the purposes of or in connection with any legal proceedings or Inquiries Act proceedings which (in any manner)—*
>
> *(a) discloses, in circumstances from which its origin in interception-related conduct may be inferred— (i) any content of an intercepted communication, or (ii) any secondary data obtained from a communication, or*
>
> *(b) tends to suggest that any interception-related conduct has or may have occurred or may be going to occur.*

What are the problems and what can you do?

1. Major modifications to a warrant should be authorised by a Judicial Commissioner.

The changes which will be permitted by use of a **major modification** have the potential to **completely change key components** of a warrant.

The warrant will initially have been reviewed and approved by a Judicial Commissioner, but requests to make major modifications are not presented to them. This is a flaw and fails the transparency and clarity test which has been set for this Bill.

The lack of authorisation by a Judicial Commissioner was **criticised** by the **Joint Committee on the Investigatory Powers Bill:**

> *"The Committee believes that this response fails to recognise that a modification, as currently worded in the draft Bill, might include adding a whole new set of people or premises to an existing warrant. The warrant could therefore be changed in a substantial way without any judicial oversight."*[4]

The process of modifying a targeted interception warrant raised the most concern amongst the Joint Committee who recommended that "major modifications for targeted interception warrants….should also be authorised by a Judicial Commissioner."

The Home Office did not accept this recommendation claiming that it would "drastically reduce the operational agility of the agencies".

Interception powers can however be used by the police and the intelligence agencies. If a major warrant can fundamentally alter the nature of the investigation it is critical that those changes be subject to a independent Judicial authorisation.

[4] Joint Committee on the draft Investigatory Powers Bill, *Report*, 3rd February 2016, p.15: http://www.publications.parliament.uk/pa/jt201516/jtselect/jtinvpowers/93/93.pdf

Other major modifications involving powers for use by the agencies are subject to approval by a Judicial Commissioner. For clarity, continuity and transparency we propose that any major modification be subject to independent authorisation by a Judicial Commissioner.

2. Material gained through interception should be used as evidence in court.

The continued ban on using **intercepted material as evidence** is nonsensical. The UK is the only Western country that follows this system. Given that this Bill allows for evidence from equipment interference to be made available as evidence in court, the argument that intercept as evidence would reveal too much about the capabilities of the intelligence agencies is another disparity which requires further explanation.

The use of material gained through interception in court has been suggested by individuals such as David Anderson QC; the Government's Independent Reviewer of Terrorism Legislation[5] and Stuart Osborne, former Senior National Coordinator of Counter Terrorism and Head of Counter Terrorism Command[6]. Currently the UK's position on it is at odds with countries such as the US, Australia and New Zealand.

[5] Joint Committee on the Draft Enhanced Terrorism Prevention and Investigation Measures Bill, Report, 27th November 2012, p. 28: http://www.publications.parliament.uk/pa/jt201213/jtselect/jtdraftterror/70/70.pdf p. 28
[6] Ibid pg.29

BIG BROTHER WATCH
DEFENDING CIVIL LIBERTIES, PROTECTING PRIVACY

Bulk Powers

Relevant Sections of the Bill

Part 5: Equipment Interference
Part 6, Chapter 1: Bulk Interception Warrants
Part 6, Chapter 2: Bulk Acquisition Warrants
Part 6, Chapter 3: Bulk Equipment Interference Warrants
Part 7: Bulk Personal Datasets

Our Recommendations

1. Bulk Equipment interference should be removed from the Bill.
2. Targeted Equipment Interference should be more tightly defined.
3. Clarity should be provided on what constitutes a Specific Bulk Personal Dataset.
4. Class Bulk Personal Datasets should be removed from the Bill.
5. The role of Judicial Commissioners in relation to Bulk Personal Datasets should be made clear on the face of the Bill.

What does the Bill say and do?

The Bill avows the use of surveillance powers in bulk by the Intelligence Agencies.

Bulk powers are one of the most controversial aspects of the Bill. Bulk by its very nature is a broad capability. It is not used against known targets but is used as *"an intelligence gathering capability."* [7]

Part 6 of the Interception of Communications draft Code of Practice accompanying the Bill states:

"If the requirements of this chapter [chapter 6] are met then the interception of all communications transmitted on a particular route or cable, or carried by a particular CSP (Communications Service Provider), could, in principle, be lawfully authorised."[8]

7. Home Office, *Interception of Communications draft Code of Practice,* p.39 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/504234/Interception_draft_code_of_practice.PDF
8. Home Office, *Interception of Communications draft Code of Practice*, p. 39: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/504234/Interception_draft_code_of_practice.PDF

Outline of Bulk Powers

Bulk Interception

Bulk Interception is described in the Bill at **Part 6, Chapter 1, Section 119, Clause 4** as:

> *(a) the interception, in the course of their transmission by means of a telecommunication system, of communications described in the warrant;*
> *(b) the obtaining of secondary data from communications transmitted by means of such a system and described in the warrant;*
> *(c) the selection for examination, in any manner described in the warrant, of intercepted content or secondary data obtained under the warrant;*
> *(d) the disclosure, in any manner described in the warrant, of anything obtained under the warrant to the person to whom the warrant is addressed or to any person acting on that person's behalf.*

The **Bill** goes on to state at **Clause 5(i)** that a bulk interception warrant also authorises the following conduct:

> *(i) the interception of communications not described in the warrant.*

Part 6 of The Interception of Communications draft Code of Practice accompanying the Bill provides more clarity.

> *"This interception will result in the collection of large volumes of communications and/or data."*

It goes on to say:

"a bulk interception warrant instrument need not name or describe the interception subject or set of premises in relation to which the interception is to take place. Neither does Chapter 1 of Part 6 impose a limit on the number of communications – which may be intercepted."

This power is intended to be used mainly as a means of monitoring internet activity of international targets, however the nature of the internet may mean that a UK citizen's data is caught up in the net of bulk interception. If the agencies wish to view the data of a UK citizen (whether based here or abroad) they must apply for a targeted examination warrant.

Bulk Acquisition

Bulk Acquisition is the power to acquire communications data in bulk from a Telecommunications Service. This power can be used against individuals in the UK.

The power is outlined in the Bill in **Part 6, Chapter 2, Sub-Sections 138(5) and (6)**

> *(6) A bulk acquisition warrant is a warrant which authorises or requires the person to whom it is addressed to secure, by any conduct described in the warrant, any one or more of the activities in subsection (7).*
>
> *(7) The activities are—*
> *(a) requiring a telecommunications operator specified in the warrant—*
> *(i) to disclose to a person specified in the warrant any communications data which is specified in the warrant and is in the possession of the operator,*
> *(ii) to obtain any communications data specified in the warrant which is not in the possession of the operator but which the operator is capable of obtaining, or*
> *(iii) to disclose to a person specified in the warrant any data obtained as mentioned in sub-paragraph (ii),*
> *(b) the selection for examination, in any manner described in the warrant, of communications data obtained under the warrant,*
> *(c) the disclosure, in any manner described in the warrant, of such data to the person to whom the warrant is addressed or to any person acting on that person's behalf.*

Bulk Equipment Interference

Bulk Equipment Interference can be found in **Part 6, Chapter 3, Section 154, Clause 1 (c)** (please note Equipment Interference is a term used for the process of hacking a device; computer, mobile phone, tablet etc.)

> *(1) For the purposes of this Act, a warrant is "bulk equipment interference warrant" if—*
> *(a) it is issued under this Chapter,*
> *(b) it authorises or requires the person to whom it is addressed to secure interference with any equipment for the purpose of obtaining—*
> *(i) communications (see section 173);*
> *(ii) equipment data (see section 155);*
> *(iii) any other information;*
> *(c) the main purpose of the warrant is to obtain one or more of the following—*
> *(i) overseas-related communications;*
> *(ii) overseas-related information;*
> *(iii) overseas-related equipment data.*

Further detail about Bulk Equipment Interference (EI) is given in **the Operational Case for Bulk Powers** which accompanies the Bill.

"A bulk EI warrant is likely required in circumstances where the Secretary of State or Judicial Commissioner is not be (SIC) able to assess the necessity and proportionality to a sufficient degree at the time of issuing the warrant."

It is worth noting that the Bill also enables Equipment Interference for the agencies and the Police in **Part 5 of the Bill**. Part 5 deals specifically with what is defined in the Bill as **Targeted Equipment Interference.** However **the Operational Case for Bulk Powers** offers further guidance which states clearly that a targeted Equipment Interference Warrant can be used in a thematic way, i.e. as a power which will enable the hacking of a group of people, a number of organisations or a broad range of locations.

Bulk Personal Datasets

Bulk Personal Datasets are outlined in **Part 7, Section 174, Subsections 1 and 2** of the Bill

> *(1) For the purposes of this Part, an intelligence service retains a bulk personal dataset if—*
>
> *(a) the intelligence service obtains a set of information that includes personal data relating to a number of individuals,*
>
> *(b) the nature of the set is such that the majority of the individuals are not, and are unlikely to become, of interest to the intelligence service in the exercise of its functions,*
>
> *(c) after any initial examination of the contents, the intelligence service retains the set for the purpose of the exercise of its functions, and*
>
> *(d) the set is held, or is to be held, electronically for analysis in the exercise of those functions.*
>
> *(2) In this section, "personal data" has the same meaning as in the Data Protection Act 1998 except that it also includes data relating to a deceased individual where the data would be personal data within the meaning of that Act if it related to a living individual.*

The Security and Intelligence Agencies' retention and use of Bulk Personal Datasets draft Code of Practice states that a Bulk Personal Dataset

"includes personal data relating to a number of individuals, and the nature of that set is such that the majority of individuals contained within it are not, and are unlikely to become, of interest to the Security and Intelligence Agencies in the exercise of their statutory functions"

Bulk Personal Datasets will be made up of data relating to UK and international people.

Bulk Personal Datasets are defined in two ways; **specific and class**. These are outlined **in Part 7, Sections 177 and 178** of the Bill. But the definitions are better explained in the **Security and Intelligence Agencies' retention and use of Bulk Personal Datasets draft Code of Practice**:

"Class BPD warrants will authorise the retention and use of a particular class of BPD. Class BPD warrants are for those datasets which are similar in their content and proposed use and raise similar considerations as to, for instance, the degree of intrusion and sensitivity, and the proportionality of using the data."

A **specific Bulk Personal Dataset** is described in the same **draft Code of Practice** as a warrant that would authorise "*a Security and Intelligence Agency to retain, or to retain and examine, the particular BPD described in the warrant*".

Warrantry process of bulk powers:

Each of these powers must have a warrant before they can be used. In all cases, other than bulk personal datasets, the warrants are authorised by the Secretary of State and "reviewed" and "approved" by a Judicial Commissioner.

For more information about warrants please see our warrants factsheet here.

What are the problems and what can you do?

1. Bulk Equipment interference should be removed from the Bill.

The **definitions and use of Bulk Equipment Interference** as outlined in the **draft Code of Practice** clearly states that this power is authorised when the **necessity and proportionality is unknown**.

This **contradicts the Home Secretary** who has been very clear throughout that powers are only used when necessary and proportionate. Indeed she stated in the House on November 11th 2015 when the draft Bill was published that her role as Secretary of State in authorising warrants required her to be *"satisfied that an activity is necessary and proportionate before a warrant can be issued."*

The lack of necessity and proportionality in relation to Bulk Equipment Interference poses a significant threat to the privacy and security of all citizens here and abroad. Bulk Equipment Interference should be removed from the Bill.

3. Clarity should be provided on what constitutes a Specific Bulk Personal Dataset and confirmation that medical records are not included must be given.

Bulk Personal Datasets (BPD) as a whole raise profound concern for the privacy of all UK citizens.

We have raised concern since the publication of the draft Bill that the definition of a Bulk Personal Dataset as a dataset which holds the personal data of people who are *"unlikely to be of intelligence interest"* appear to create a secondary purpose for datasets that we find ourselves on purely by being born and living in the UK.

Before this Bill is passed it is important that BPDs are better defined and that reassurance is provided that they do not, and will not, contain data relating to people's medical records.

4. Class Bulk Personal Datasets should be removed from the Bill.

Whilst those specific datasets are a profound concern the broadness of a Class Bulk Personal Dataset raises another level of concern. It is unclear under what circumstances a warrant to collect a Class Bulk Personal Dataset could be defined as either necessary or proportionate. The Security and Intelligence Agencies retention and use of bulk personal datasets code of practice makes clear that a class warrant would be issued to allow the intelligence agencies to gather datasets of a similar nature in bulk.

The **Joint Committee** recommended that *"authorisations for bulk personal datasets should be required to be specific and provisions for class authorisations should be removed from the Bill."*

The **Intelligence and Security Committee** noted that *"the acquisition, retention and examination of any Bulk Personal Dataset is sufficiently intrusive that it should require a specific warrant. We therefore recommend that Class Bulk Personal Dataset warrants are removed from the new legislation."*

The Home Office did not accept either recommendation. **Class Bulk Personal Datasets are too broad. We support the recommendations by the Joint Committee and the Intelligence and Security Committee and recommend that Parliament look again at the recommendations and seek amendments to the Bill.**

5. The role of Judicial Commissioners in relation to Bulk Personal Datasets should be made clear on the face of the Bill.

The privacy safeguards for UK citizens present on Bulk Personal Datasets are weak and need work to ensure that citizens are properly protected. The draft Code of Practice on BPDs notes that there is no process for Judicial Commissioners to record their decision on the acquisition of a BPD, this poses serious questions about the transparency of BPDs and the nature of their use.

New sections should be added to the Bill to outline what role the Judicial Commissioners will have in overseeing how Bulk Personal Datasets are used by the intelligence agencies.

BIG BROTHER WATCH
DEFENDING CIVIL LIBERTIES, PROTECTING PRIVACY

Equipment Interference

Relevant Sections of the Bill

Part 5: Equipment Interference

Our recommendations

1. The authorisation process for Equipment Interference warrants should be the same for each organisation.
2. Targeted Equipment Interference should be more tightly defined.

What does the Bill say and do?

Authorisation

The Bill creates two separate authorisation processes for Equipment Interference:

The Secretary of State will authorise the warrants requested by the intelligence agencies as outlined in **Part 5, Section 91: Power to issue warrants to intelligence services: the Secretary of State**

> *(1) The Secretary of State may, on an application made by or on behalf of the head of an intelligence service, issue a targeted equipment interference warrant if—*
>
> *(a) the Secretary of State considers that the warrant is necessary on grounds falling within subsection (5),*
>
> *(b) the Secretary of State considers that the conduct authorised by the warrant is proportionate to what is sought to be achieved by which conduct,*
> *(c) the Secretary of State considers that satisfactory arrangements made for the purposes of sections 112 and 113 (safeguards relating to disclosure etc.) are in force in relation to the warrant, and*
> *(d) except where the Secretary of State considers that there is an urgent need to issue the warrant, the decision to issue the warrant has been approved by a Judicial Commissioner*

Warrants for law enforcement agencies however are authorised by a "*law enforcement chief*". There has been no explanation as to why this is the case. **Part 5, Section 96** outlines this

> *(1) A law enforcement chief described in Part 1 or 2 of the table in Schedule 6 may, on an application made by a person who is an appropriate law enforcement officer in relation to the chief, issue a targeted equipment interference warrant if—*
>
> *(a) the law enforcement chief considers that the warrant is necessary for the purpose of preventing or detecting serious crime,*
> *(b) the law enforcement chief considers that the conduct authorised by the warrant is proportionate to what is sought to be achieved by that conduct,*

> *(c) the law enforcement chief considers that satisfactory arrangements made for the purposes of sections 112 and 113 (safeguards relating to disclosure etc.) are in force in relation to the warrant, and*
> *(d) except where the law enforcement chief considers that there is an urgent need to issue the warrant, the decision to issue it has been approved by a Judicial Commissioner.*

Additionally **Subsection 96(7)** mandates that HMRC follow the process for law enforcement agencies and don't apply to a Secretary of State for a warrant:

> (*8) A law enforcement chief who is an officer of Revenue and Customs may consider that the condition in subsection (1)(a) is satisfied only if the serious crime relates to an assigned matter within the meaning of section 1(1) of the Customs and Excise Management Act 1979.*

Similarly the Competition and Markets Authority also follow the same procedure:

> *(9) A law enforcement chief who is the chair of the Competition and Markets Authority may consider that the condition in subsection (1)(a) is satisfied only if the offence, or all of the offences, to which the serious crime relates are offences under section 188 of the Enterprise Act 2002*

Thematic Warrants

Part 5, Section 90 of the Bill allows for a targeted warrant to be deployed against organisations, specific locations or groups of individuals with a common purpose. This is less targeted and more thematic in nature.

The Operational Case for Bulk Powers outlines how a targeted warrant can be used in a bulk way by referring to a targeted warrant as a *"targeted thematic warrant"*

> *"Both bulk EI and targeted 'thematic' EI operations can take place at scale, if the relevant criteria are met. It is entirely possible for a targeted 'thematic' EI warrant to cover a large geographic area or involve the collection of a large volume of data."*[9].

The word **"thematic"** relation to **Equipment Interference does not appear anywhere on the face of the Bill,** it is only hinted at in **Part 5, Section 90**:

> *(1) A targeted equipment interference warrant may relate to any one or more of the following matters—*
> *(a) equipment belonging to, used by or in the possession of a particular person or organisation;*
> *(b) equipment belonging to, used by or in the possession of a group of persons who share a common purpose or who carry on, or may carry on, a particular activity;*

[9] Home Office, *Operational Case for Bulk Powers* p. 31: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/504187/Operational_Case_for_Bulk_Powers.pdf

(c) equipment belonging to, used by or in the possession of more than one person or organisation, where the interference is for the purpose of a single investigation or operation;
(d) equipment in a particular location;
(e) equipment in more than one location, where the interference is for the purpose of the same investigation or operation;
(f) equipment which is being, or may be used, for the purposes of a particular activity or activities of a particular description;
(g) equipment which is being, or may be used, to test, maintain or develop capabilities relating to interference with equipment for the purpose of obtaining communications, equipment data or other information;
(h) equipment which is being, or may be used, for the training of persons who carry out, or are likely to carry out, such interference with equipment.

What are the problems and what can you do?

1. The authorisation process for Equipment Interference warrants should be the same for each organisation.

The system for the authorisation of targeted Equipment Interference is not the same for each organisation. Currently the Secretary of State will authorise the warrants requested by the intelligence agencies and "*law enforcement chief*" will do the same for organisations such as police forces. There has been no explanation for this difference and at present all it does is cause unnecessary confusion.

The Bill should be amended to make both authorisation processes the same. Much has been made of the "*double-lock*" system of both Secretary of State and Judicial Commissioner. It should be the case that it is applied consistently.

2. Targeted Equipment Interference should be more tightly defined.

Both the Joint Committee and the Intelligence and Security raised concern about this.

The **Joint Committee** stated that *"the language of the Bill be amended so that....targeted equipment interference warrants cannot be used as a way to issue thematic warrants concerning a very large number of people."*

Whilst the **Intelligence and Security Committee** recommended that *"the new legislation should require the Agencies to obtain a Targeted Equipment Interference warrant for an operation overseas whenever it is practical to do so."*

The Home Office did not accept either recommendation.

Targeted Equipment Interference should be rewritten to ensure that any thematic use of the Power should be clearly defined on the face of the Bill.

BIG BROTHER WATCH
DEFENDING CIVIL LIBERTIES, PROTECTING PRIVACY

Safeguards

Relevant Sections of the Bill

Part 8, Chapter 1: Investigatory Powers Commissioner and other Judicial Commissioners

Our recommendations

1. A real "double lock" system for the authorisation of warrants should be introduced.
2. Judicial Commissioners should be appointed by the Judicial Appointments Committee.
3. Discussions about the staffing, funding and resourcing of the IPC should be open to a broad range of individuals and organisations.
4. Proposals for user notification should be strengthened to create a system that brings real redress.
5. The Bill should be subject to annual Parliamentary review.

What does the Bill say and do?

The Bill attempts to provide a number of safeguards throughout the Bill.

Investigatory Powers Commission

A new oversight body**, The Investigatory Powers Commission (IPC)**, will replace the current Commissioners, meaning that the following bodies will be abolished:

Part 8, Chapter 1, Section 206 Abolition of existing oversight bodies

(1) The offices of the following are abolished—
(a) the Interception of Communications Commissioner,
(b) the Intelligence Services Commissioner,
(c) the Investigatory Powers Commissioner for Northern Ireland,
(d) the Chief Surveillance Commissioner,
(e) the other Surveillance Commissioners,
(f) the Scottish Chief Surveillance Commissioner, and
(g) the other Scottish Surveillance Commissioners.

The Prime Minister will have the power to appoint both the Investigatory Powers Commissioner and the Judicial Commissioners.

Part 8, Chapter 1, Section 194 Investigatory Powers Commissioner and other Judicial Commissioners

> *(1) The Prime Minister must appoint—*
> *(a) the Investigatory Powers Commissioner, and*
> *(b) such number of other Judicial Commissioners as the Prime Minister considers necessary for the carrying out of the functions of the Judicial Commissioners.*

Subsection 3 requires the Prime Minister to consult a number of individuals in both the judiciary and the devolved administration before finalising any appointments:

> *(3) Before appointing any person under subsection (1), the Prime Minister must consult—*
> *(a) the Lord Chief Justice of England and Wales,*
> *(b) the Lord President of the Court of Session,*
> *(c) the Lord Chief Justice of Northern Ireland,*
> *(d) the Scottish Ministers, and (e) the First Minister and deputy First Minister in Northern Ireland.*

The staffing and resourcing of the new body will be decided by the Secretary of State, who is required to consult with the Investigatory Powers Commissioner.

Part 8, Chapter 1, Section 204 Funding, staff and facilities

> *(1) There is to be paid to the Judicial Commissioners out of money provided by Parliament such remuneration and allowances as the Treasury may determine.*
> *(2) The Secretary of State must, after consultation with the Investigatory Powers Commissioner and subject to the approval of the Treasury as to numbers of staff, provide the Judicial Commissioners with—*
> *(a) such staff, and*
> *(b) such accommodation, equipment and other facilities, as the Secretary of State considers necessary for the carrying out of the Commissioners' functions.*

Judicial Double Lock

Most warrants will now be subject to a two stage process defined by the Home Secretary as a "double lock" system. In the majority of cases this will involve both a Secretary of State and a Judicial Commissioner.

Using the process of authorising an interception warrant as an example a warrant is signed off by a Secretary of State in the first instance:

Part 2, Chapter 1, Section 17: Power of Secretary of State to issue warrants

(1) The Secretary of State may, on an application made by or on behalf of an intercepting authority mentioned in section 16(1)(a) to (g), issue a targeted interception warrant if—

(a) the Secretary of State considers that the warrant is necessary on grounds falling within section 18,

(b) the Secretary of State considers that the conduct authorised by the warrant is proportionate to what is sought to be achieved by that conduct,

(c) the Secretary of State considers that satisfactory arrangements made for the purposes of sections 46 and 47 (safeguards relating to disclosure etc.) are in force in relation to the warrant, and

(d) except where the Secretary of State considers that there is an urgent need to issue the warrant, the decision to issue the warrant has been approved by a Judicial Commissioner. This is subject to subsection (5).

Section 21 of the same Chapter goes onto require the authorised warrant be sent to a Judicial Commissioner who will decide whether or not to approve it, based on a system of judicial review:

Part 2, Chapter 1, Section 21: Approval of warrants by Judicial Commissioners

(1) In deciding whether to approve a person's decision to issue a warrant under this Chapter, a Judicial Commissioner must review the person's conclusions as to the following matters—

(a) whether the warrant is necessary on relevant grounds (see subsection (3)), and

(b) whether the conduct that would be authorised by the warrant is proportionate to what is sought to be achieved by that conduct.

(2) In doing so, the Judicial Commissioner must apply the same principles as would be applied by a court on an application for judicial review.

(3) In subsection (1)(a) "relevant grounds" means—

(a) in the case of a warrant to be issued by the Secretary of State, grounds falling within section 18;

(b) in the case of a warrant to be issued by the Scottish Ministers, grounds falling within section 19(4).

(4) Where a Judicial Commissioner refuses to approve a person's decision to issue a warrant under this Chapter, the Judicial Commissioner must give the person written reasons for the refusal.

(5) Where a Judicial Commissioner, other than the Investigatory Powers Commissioner, refuses to approve a person's decision to issue a warrant under this Chapter, the person may ask the Investigatory Powers Commissioner to decide whether to approve the decision to issue the warrant.

For more information about authorisation please see our factsheet here.

Error reporting

Part 8, Chapter 1, Section 198 of the Bill deals with **Error Reporting**, the Bill states:

Clause 1 states

"The Investigatory Powers Commissioner must inform a person of any relevant error relating to that person of which the Commissioner is aware of the Commissioner considers that -

(a) the error is a serious error, and

(b) It is in the public interest for the person to be informed of the error

Clause 3 states

"Accordingly, the fact that there has been a breach of a person's Convention rights (within the meaning of the Human Rights Act 1998) is not sufficient by itself for an error to be a serious error."

Clause 4 states:

"*In making a decision under subsection (1)(b), the Investigatory Powers Commissioner must, in particular, consider—*

(a) the seriousness of the error and its effect on the person concerned, and

(b) the extent to which disclosing the error would be contrary to the public interest or prejudicial to—

(i) national security,

(ii) the prevention or detection of serious crime,

(iii) the economic well-being of the United Kingdom, or

(iv) the continued discharge of the functions of any of the intelligence services."

Clause 5 states:

"*Before making a decision under subsection (1)(a) or (b), the Investigatory Powers Commissioner must ask the public authority which has made the error to make submissions to the Commissioner about the matters concerned.*"

Clause 6 states:

"*When informing a person under subsection (1) of an error, the Investigatory Powers Commissioner must—*

(a) inform the person of any rights that the person may have to apply to the Investigatory Powers Tribunal, and

(b) provide such details of the error as the Commissioner considers to be necessary for the exercise of those rights, having regard in particular to the extent to which disclosing the details would be contrary to the public interest or prejudicial to anything falling within subsection (4)(b)(i) to (iv)."

Review of operation of the Act

The Bill states in **Part 9, Section 2, Clause 222 t**hat Home Secretary is required to prepare a report on the operation of the Act.

> *(1) The Secretary of State must, within the period of 6 months beginning with the end of the initial period, prepare a report on the operation of this Act.*
> *(2) In subsection (1) "the initial period" is the period of 5 years and 6 months beginning with the day on which this Act is passed.*
> *(3) In preparing the report under subsection (1), the Secretary of State must, in particular, take account of any report on the operation of this Act made by a Select Committee of either House of Parliament (whether acting alone or jointly).*
> *(4) The Secretary of State must—*
> *(a) publish the report prepared under subsection (1), and*
> *(b) lay a copy of it before Parliament.*

What are the problems and what can you do?

1. A real "double lock" system for the authorisation of warrants should be introduced.

The proposed "double-lock" system of authorising warrants doesn't specify a specific definition of judicial review nor is it consistently applied across each power.

The Bill clearly states that Judicial Commissioners will have to apply the same principles to the decision as they would to a "*judicial review*". Throughout the evidence given to the Joint

Committee scrutinising the Bill, numerous differing definitions of what "review" might mean were provided. No clarity was determined.

In **his evidence to the Joint Committee** scrutinising the Bill **Martin Chamberlain QC** raised concern with the presence of the phrase in the Bill:

> "*The problem with simply saying that the standard to be applied is judicial review is that we do not know what arguments the Government will make to the judicial commissioners, and it is quite possible that the Government will say that this is the context, balancing the needs of national security against the intrusion into privacy, where you have to accord considerable latitude and discretion to the elected Minister, and where the judge really should not interfere, unless the Minister has obviously struck the wrong balance.*"

The way the "double lock" has been defined indicates that the Judicial Commissioner would be asked to "review" and "approve" an existing decision, rather than be given the opportunity to independently assess the warrant without prejudice of a pre-existing determined authorisation.

This process therefore is less "double lock" more "rubber stamp" of approval. Particularly when it is noted throughout the Bill that should a Judicial Commissioner disagree with the authorisation, the Secretary of State can go above their head and seek "review" and "approval" from the Investigatory Powers Commissioner instead, thereby undermining the Judicial Commissioners decision.

It is worth noting that in 2014 the Home Secretary signed off 2,345 interception warrants, equivalent to 6 every day. When you consider that with the continued expansion of the Internet of Things more and more data will be become available, the system being proposed may see the Secretary of State become little more than an authorising machine for warrants, with little time to dedicate to her wider responsibilities.

A double lock should describe the process of independent authorisation, not a process of a Judicial Commissioner reviewing and approving an authorisation by a Secretary of State. Members of Parliament should consider further what the impact a "double lock" of this nature will have on the role of the Home Secretary long term.

2. Judicial Commissioners should be appointed by the Judicial Appointments Committee

Allowing the Prime Minister to appoint the Commissioners will concentrate too much power in the hands of the Executive. This could damage the independence of the body before it is even established.

Commissioners should be appointed by the Judicial Appointments Committee (JAC). This would give the IPC more independence as well as credibility as an oversight body. The Bill should be amended to ensure this happens.

3. Discussions about the staffing, funding and resourcing of the IPC should be open to a broad range of individuals and organisations

Although the Treasury will have the final say on what funding the IPC receives the Bill also gives the Secretary of State the power to arrive at a figure based on consultation with only the Investigatory Powers Commissioner. This runs the risk of a decision being taken with little or no real consultation.

The staffing and resourcing of the body will be crucial to determining its effectiveness. It is important that a wide selection of groups and individuals are involved in discussions about this. Members of Parliament should amend the Bill to make sure a multiple views are taken into account.

4. Proposals for error reporting should be strengthened to create a system that brings real redress for innocent people.

The Bill does not provide the opportunity for genuine redress to innocent people who may have been wrongly surveilled using any of the powers outlined in the Bill.

The wording of the Bill states that an individual can only be informed of a serious error if it is in the public interest to do so.

We believe that with work it is entirely possible for **Section 198** to be amended to allow the Investigatory Powers Commissioner the ability to inform innocent people who have been wrongly surveilled the right to redress without having to detail the specifics of the case in a way which would impact the work of the agencies, much like the proposed use for Equipment Interference as evidence.

The Bill already makes provision for the Investigatory Powers Commissioner to *"provide such details of the error as the Commissioner considers to be necessary for the exercise of those rights."* Were the requirements for national security concerns and the continued discharge of the functions of any of the intelligence agencies not to be revealed to the individual we feel that there is an opportunity for redress to be sought adequately.

It is critical that an individual wrongly surveilled can be informed of the error and be given the opportunity to seek redress. An alternative solution which protects national security and the work of the intelligence agencies whilst enabling notification of error should be established

5. The Bill should be subject to the same review as the National Security Strategy and Strategic Defence Review

In light of the fact that technology continues to move apace, it is critical that laws which involve surveillance and interception of those technologies is up to date and subject to review.

The Bill is written in part in a way that is designed to "futureproof" its capabilities. This makes for broad and loosely defined legislation.

Because the Bill deals with issues regarding National Security it should be subject to the same process as the National Security Strategy and Strategic Defence Review, not the process of internal review undertaken by the Home Secretary as proposed in the Bill. This will not be strong enough and will not allow for clear oversight and transparency by Parliament.

This will bring proper scrutiny and ensure that the law remains relevant and accurate.

BIG BROTHER WATCH
DEFENDING CIVIL LIBERTIES, PROTECTING PRIVACY

About Big Brother Watch

Big Brother Watch is a civil liberties and privacy campaign group founded in 2009. We produce unique research which exposes the erosion of civil liberties in the UK, looks at the dramatic expansion of surveillance powers, the growth of the database state and the misuse of personal information. We have engaged with a number of Parliamentary Committees on these issues.

We have been active in campaigning on the issues of mass surveillance and privacy for a number of years **and gave both written and oral evidence to the Joint Committee on the Draft Investigatory Powers Bill**. Additionally we **gave written evidence to both the Science and Technology Committee's** inquiry into the technical aspects of the draft Bill **and the Joint Committee on Human Right's** process of pre-legislative scrutiny.