Home Office

Home Secretary

2 Marsham Street,
London SW1P 4DF
www.gov.uk/home-office

Rt Hon Dominic Grieve QC MP
Intelligence and Security Committee
35 Great Smith Street
London
SW1P 3BQ

8 December 2015

Dear Dominic

As promised in response to your question following my statement to the House on the draft Investigatory Powers Bill, please find enclosed herein supplementary material to the Government's formal response to the report of the previous Intelligence and Security Committee of Parliament on Privacy and Security which it published in March this year.

As I and the Prime Minister have both publically stated, the draft Investigatory Powers Bill should be considered as the formal Government response to that report. I do, however, acknowledge that the previous Committee's report covered topics that the draft bill does not account for and I can understand your concern that there has therefore been no formal response to these recommendations. As such, I attach two supplementary documents which together, address all of the recommendations and conclusions in that Committee's report;

(a) the Government response to the small number of recommendations and conclusions not addressed by the draft Investigatory Powers Bill; and
(b) a summary of how the draft Bill addresses the majority of the recommendations and conclusions in the report (a previous iteration of which was provided to your Secretariat)

I hope these assist you in understanding how this Government has given careful consideration to the very valuable work conducted by the previous Committee, and that provided by the reviews of David Anderson QC, and the Royal United Services Institute and our ongoing commitment to openness and transparency.

I will be placing copies of this letter and the accompanying documents in the House Library and also hope you will consider publishing them on your website alongside your original report.

Yours sincerely

Rt Hon Theresa May MP

GOVERNMENT RESPONSE TO THE ISC REPORT ON PRIVACY AND SECURITY

The Intelligence and Security Committee of Parliament (ISC) published its report into Privacy and Security on 12 March 2015. In a written statement to Parliament, the Prime Minister stated that "*We will consider the ISC's findings and recommendations carefully. As a number of these are currently the subject of related reviews, including by the Independent Reviewer of Terrorism Legislation, the Government's intention is to review all the recommendations and suggestions in a full and considered manner before making a substantive response."*

As the draft Investigatory Powers Bill has now been published, the Government is able to respond formally to the ISC's report and address those recommendations and conclusions not covered in the draft bill.

The Government accepted and agrees with the ISC's overarching recommendation for a new piece of legislation which must "*clearly set out the intrusive powers available to the Agencies, the purposes for which they may use them, and the authorisation required before they may do so".* The draft Bill provides a comprehensive and comprehensible framework governing the acquisition of communications, data about communications, and equipment interference.

Further, the Government accepts and agrees with the vast majority of the detailed recommendations and conclusions in the report. This response, together with the draft Investigatory Powers Bill, forms the substantive response to the Report. For completeness, Annex A provides a breakdown for each recommendation or conclusion that is relevant to the draft Bill.

A small number of recommendations and conclusions lie outside the scope of the draft Bill. The Government response to those is below.

Z: The Agencies conduct both 'Intrusive Surveillance' (typically inside a private residence or vehicle) and 'Directed Surveillance' (typically conducted in public places). These are targeted capabilities, involving considerable resources, and as a consequence are used sparingly.

Z: The Government acknowledges the ISC's conclusion that these targeted capabilities are used sparingly. They are only used where it is necessary and proportionate to do so and where the activity has been properly authorised.

AA. Where the Agencies interfere with property and wireless telegraphy in the UK, they obtain specific Ministerial authority in the form of a warrant under Section 5 of the Intelligence Services Act 1994. However, we note that in certain circumstances the Agencies gain access to an SoI's property under the authority of another organisation's warrant. This practice – while legal – should be subject to greater oversight by both Ministers and the Intelligence Services Commissioner.

AA: The Government acknowledges the conclusion that when the Agencies gain access to an SoI's property this is done legally under a warrant. Any warrant used to authorise such action is signed by a Secretary of State, this will remain the case. Such warrants are currently subject to oversight by the Intelligence Services Commissioner. The proposed new Investigatory Powers Commissioner will have a broad remit and may look at any use of investigatory power by a public authority that he or she thinks is deserving of additional scrutiny and oversight.

The draft Bill makes clear that the Commissioner can undertake investigations, report at any time and have access to any information.

BB. While intrusive action within the UK requires a Ministerial warrant, outside the UK it is authorised by use of a Class Authorisation under the Intelligence Services Act 1994. However, the Agencies do not all keep detailed records of operational activity conducted under these Class Authorisations. It is essential that they keep comprehensive and accurate records of when they use these powers. It is unacceptable not to record information on intrusive action.

OO. Section 7 of the Intelligence Services Act 1994 allows for a Secretary of State to sign an authorisation which removes civil and criminal liability for activity undertaken outside the British Islands which may otherwise be unlawful under UK law. We have examined the Class Authorisations allowed under ISA in detail and are satisfied that they are required in order to allow the Agencies to conduct essential work. Nevertheless, that may involve intruding into an individual's private life, and consideration should therefore be given to greater transparency around the number and nature of Section 7 Authorisations.

PP. We consider that Ministers must be given greater detail as to what operations are carried out under each Class Authorisation: a full list should be provided every six months. We also recommend that Ministers provide clear instructions as to what operations they would expect to be specifically consulted on, even if legally no further authorisation would be required.

BB, OO and PP: As with all authorisations obtained under section 7 of the Intelligence Services Act 1994 (ISA), the class authorisations are subject to review and renewal by the Secretary of State every six months. The class authorisations cover routine day-to-day business of the Agencies overseas, and as such it would be disproportionate for the Secretary of State to be informed of each instance where a class authorisation is utilised. The Intelligence Services Commissioner provides statutory oversight of all authorisations issued and renewed under section 7 of ISA and reports his findings to the Prime Minister.

The Government remains committed to greater transparency around the use of investigatory powers as the recent publication of the Transparency Report demonstrates. However, the Government believes that disclosure of specific details of the class authorisations would be damaging to national security as they relate to sensitive capabilities and activities.

In response to recommendation BB (and to a recommendation made by the Intelligence Services Commissioner in his 2014 Annual Report) SIS have launched a review of their use of class authorisations to strengthen existing arrangements and to enhance their ability to demonstrate compliance in a more systematic way.

The Agencies will when necessary seek a specific authorisation for a proposed operation or activity overseas where such activity is not covered by a class authorisation. In addition, and in line with long-standing practice, regardless of whether a class authorisation could be applied, the Agencies will in all cases seek specific Ministerial authorisation for any proposed activity likely to carry significant political risk

DD. GCHQ need to be able to read the encrypted communications of those who might pose a threat to the UK. We recognise concerns that this work may expose the public to greater risk and could have potentially serious ramifications (both political and economic). We have questioned GCHQ about the risks of their work in this area. They emphasised that much of their work is focused on improving security online. In the limited circumstances where they do * they would only do so where they are confident that it could not be ***. However, we are concerned that such decisions are only taken internally: Ministers must be kept fully informed of all such work and specifically consulted where it involves potential political and economic risks.**

DD: The Government is clear that Ministers are already kept informed of such work and are specifically consulted where it involves potentially significant political and economic risks.

EE. The Agencies have put in place internal policy guidance governing the processes and safeguards to be applied when recruiting and running agents, and detailed training to their agents about what they can and cannot do. We nevertheless consider that more should be done to assure the public that, where the Agencies 'sub-contract' intrusive activity to their agents, those agents must adhere to the same ethical standards as the Agencies themselves, and abide by the same legal framework. The Government should therefore set out a clear and transparent ethical framework describing the conduct that is expected of anyone whom the Agencies engage as an agent.

EE: The Agencies protection of agents is properly authorised and subject to high ethical standards Publishing anything which might enable someone to be identified as an agent through their behaviours would break this covenant. The activities of agents are properly authorised and currently subject to oversight by the Intelligence Services Commissioner. The new Investigatory Powers Commissioner will continue to oversee this activity.

MM. The Intelligence Services Act 1994 and the Security Service Act 1989 provide the legal basis for the Agencies' activities, and broad general powers to act in accordance with their statutory functions and purposes. We have concerns about the lack of transparency surrounding these general powers, which could be misconstrued as providing the Agencies with a 'blank cheque' to carry out whatever activities they deem necessary. We therefore recommend that the Agencies' powers are set out clearly and unambiguously.

XX. The Committee considers that the Government should introduce a new Intelligence Services Bill setting out, in one Act of Parliament, the functions of the three UK intelligence and security Agencies. This should consolidate the intelligence and security related provisions of the following legislation:

- **Security Service Act 1989;**
- **Intelligence Services Act 1994;**
- **Regulation of Investigatory Powers Act 2000;**
- **Wireless Telegraphy Act 2006;**
- **Telecommunications Act 1984;**
- **Counter-Terrorism Act 2008; and**
- **the relevant provisions of other legislation as appropriate.**

MM and XX: The Government has produced a draft Investigatory Powers Bill which provides a comprehensive and comprehensible framework governing the acquisition of communications, data about communications, and equipment interference. The purposes for which MI5, SIS and GCHQ can act are already clearly stated in the Security Service Act 1989 and the Intelligence Services Act 1994. The Government does not believe there is a need to update these, or to introduce legislation that is not related to the interference with private communications. Where the Acts listed by the ISC include provisions related to such interference, these have been consolidated into the draft Investigatory Powers Bill. The draft bill also places restrictions on the use of these Acts to obtain bulk data.

The table below provides an overview of how the Government has responded to the recommendations and conclusions in the ISC's Privacy and Security Report that are relevant to the draft Investigatory Powers Bill.

Recommendation		Government Response
A	The targeted interception of communications (primarily in the UK) is an essential investigative capability which the Agencies require in order to learn more about individuals who are plotting against the UK. In order to carry out targeted interception, the Agencies must apply to a Secretary of State for a warrant under Section 8(1) of RIPA. From the evidence the Committee has seen, the application process followed by MI5 is robust and rigorous. MI5 must provide detailed rationale and justification as to why it is necessary and proportionate to use this capability (including, crucially, an assessment of the potential collateral intrusion into the privacy of innocent people).	The Government welcomes the ISC's endorsement of the strong safeguards that apply to the targeted interception regime under existing legislation. These safeguards have been carried across to the provisions in Chapter 1 of Part 2 of the draft Investigatory Powers Bill and will be strengthened by the application of further safeguards.
B	GCHQ and SIS obtain fewer 8(1) warrants. When they do apply for such warrants, they do so via a submission to the Foreign Secretary. While this submission covers those aspects required by law, it does not contain all the detail covered by MI5's warrant applications. We therefore recommend that GCHQ and SIS use the same process as MI5 to ensure that the Home Secretary and the Foreign Secretary receive the same level of detail when considering an 8(1) warrant application.	The Government agrees that there should be consistency in processes and applications where appropriate. Part 2, Chapter 1 of the draft Bill provides a single, clear warrant granting regime and ensures consistency through the application of robust oversight and authorisation arrangements for all agencies that use interception powers. The draft Bill provides for targeted interception warrants and targeted examination warrants (clause 12). Further details will be in Codes of Practices, which will be published in draft on formal introduction of the Bill in 2016.
C	RIPA expressly prohibits any reference to a specific interception warrant. We do not consider this is proportionate: disclosure should be permissible where the Secretary of State considers that this could be done without damage to national security.	The Government recognises the importance of being as transparent as possible. The draft Bill provides for greater transparency than ever before by clarifying, within the constraints imposed by national security, the current restrictions and prohibitions relating to the disclosure of warrants and intercepted material (RIPA ss.15 and 19, Official Secrets Act 1989 s.4) in order to ensure, in particular, that: (a) there is no legal obstacle to explaining the uses (and utility) of warrants to Parliament, courts and public. Clause 43(5)(h) allows for the

		disclosure of information which does not relate to any specific warrant but relates to interception warrants in general. This will allow for the explaining of the uses and utility of warrants to Parliament, courts and the public. (b) as recommended by the Police Ombudsman for Northern Ireland in his report of 30 October 2014 on the Omagh bombing, there is "*absolute clarity as to how specific aspects of intelligence can be shared in order to assist in the investigation of crime*". Clause 40 imposes restrictions on the access to and disclosure of intercept material, limiting this to the minimum necessary for the authorised purposes. The authorised purposes include prevention or detection serious crime. This clause, in combination with s19 of the Counter-Terrorism Act 2008 (which includes provisions on the disclosure of information by the Intelligence Agencies) permits intelligence to be shared with law enforcement bodies in order to assist in the investigation of a serious crime.
D	The Agencies have described 'thematic warrants' as covering the targeted interception of the communications of a "defined group or network" (as opposed to one individual). The Committee recognises that such warrants may be necessary in some limited circumstances. However, we have concerns as to the extent that this capability is used and the associated safeguards. Thematic warrants must be used sparingly and should be authorised for a shorter timescale than a standard 8(1) warrant.	Clauses 13 and 83 of the draft Bill provide for 'thematic' warrants by enabling targeted interception and equipment interference warrants to be issued in relation to a specific operation or investigation. Such warrants will be subject to strict safeguards. Clause 23 of the draft Bill requires that operation-specific interception warrants should include details of the targets who are the subjects of those warrants. Clause 93 makes equivalent provisions in respect of equipment interference warrants. The overall warrantry authorisation regime is also being made more robust.
E	There are other targeted techniques the Agencies can use which also give them access to the content of a specific individual's communications. However, the use of these capabilities is not necessarily subject to the same rigour as an 8(1) warrant, despite providing them with the same result. All capabilities which provide the content of an individual's communications should be subject to the same legal safeguards, i.e. they must be authorised by a Secretary of State and the application to the Minister must specifically address the Human Rights Act 'triple test' of legality, necessity and proportionality.	The Government recognises the need to provide a single, clear warrant granting regime and to ensure consistency. Covert capabilities, such as the use of interception (including through Wireless Telegraphy) and equipment interference have been put on a clear statutory footing through Parts 2 and 5 of the draft Bill and will be subject to strict safeguards. Bulk interception and equipment interference powers are also available to the security and intelligence agencies and provided for in Part 6 of the draft Bill. Similar safeguards are set out in the Bill in relation to both targeted and bulk use of these powers. Ministers will be directed, through the Bill to only authorise a warrant where they are assured that it is both necessary and proportionate.

F	GCHQ's bulk interception capability is used either to investigate the communications of individuals already known to pose a threat, or to generate new intelligence leads, for example to find terrorist plots, cyber attacks or other threats to national security. It has been alleged – inaccurately – that this capability allows GCHQ to monitor all of the communications carried over the internet. GCHQ could theoretically access a small percentage (***%) of the 100,000 bearers which make up the internet, but in practice they access only a fraction of these (***%) – we detail below the volume of communications collected from these bearers. GCHQ do not therefore have 'blanket coverage' of all internet communications, as has been alleged – they have neither the legal authority, the technical capacity nor the resources to do so.	The Government welcomes the ISC's clarification that GCHQ does not have 'blanket coverage' of all internet communications, and that it only examines those communications that relate to its statutory purposes. This is provided for in Part 6 of the Bill at clauses 107 (bulk interception), 122 (bulk communications data acquisition), and 137 (bulk equipment interference) of the draft Bill. These statutory purposes are set out clearly in the draft Bill and limit examination to those situations where it is necessary in the interests of national security; for the purposes of preventing or detecting serious crime; or in the interests of the economic well-being of the UK so far as those interests are also relevant to the national security of the UK. Examination is only permitted for the statutory purpose the warrant has been issued. The draft Bill maintains the strong safeguards that apply to the bulk interception regime. It will strengthen existing statutory safeguards so that analysts will only be able to search for and examine communications where it is necessary in the pursuit of a specified operational purpose that has been authorised by the Secretary of State and approved by the Judicial Commissioner. This will apply irrespective of the person's nationality or location and will apply to both the content of communications and related communications data that may be intercepted under the bulk interception regime. Clause 119 provides that where an intelligence agency is investigating a person in the British Islands, the agency will need to obtain a targeted examination warrant under clause 12(1)(b) before it may examine the
G	It has been suggested that GCHQ's bulk interception is indiscriminate. However, one of the major processes by which GCHQ conduct bulk interception is targeted. GCHQ first choose the bearers to access (a small proportion of those they can theoretically access) and then use specific selectors, related to individual targets, in order to collect communications from those bearers. This interception process does not therefore collect communications indiscriminately.	
H	The second bulk interception process we have analysed involves the *** collection of large quantities of communications. ***. However, this collection is not indiscriminate. GCHQ target only a small proportion of those bearers they are able to access. The processing system then applies a set of selection rules and, as a result, automatically discards the majority of the traffic on the targeted bearers.	

I	There is a further filtering stage before analysts can select any communications to examine or read. This involves complex searches to draw out communications most likely to be of greatest intelligence value and which relate to GCHQ's statutory functions. These searches generate an index. Only items contained in this index can potentially be examined – all other items cannot be searched for, examined or read.	contents of that person's communications intercepted under a bulk warrant. Clause 147 applies similar safeguards in respect of data acquired under bulk equipment interference warrants.
J	Our scrutiny of GCHQ's bulk interception via different methods has shown that while they collect large numbers of items, these have all been targeted in some way. Nevertheless, it is unavoidable that some innocent communications may have been incidentally collected. The next stage of the process – to decide which of the items collected should be examined – is therefore critical. For one major method, a 'triage' process means that the vast majority (***%) of the items collected are never looked at by an analyst. For another major method, the analysts use the search results to decide which of the communications appear most relevant and examine only a tiny fraction (***%) of the items that are collected. In practice this means that fewer than *** of ***% of the items that transit the internet in one day are ever selected to be read by a GCHQ analyst. These communications – which only amount to around *** thousand items a day – are only the ones considered to be of the highest intelligence value. Only the communications of suspected criminals or national security targets are deliberately selected for examination.	The Government welcomes the ISC's conclusion that only the communications of suspected criminals or national security targets are deliberately selected for examination by GCHQ. Part 6 of the draft Bill maintains the strong safeguards that apply to the bulk interception regime and provides equivalent safeguards in respect of bulk communications data and bulk equipment interference. It strengthens existing statutory safeguards so that analysts will only be able to search for and examine communications where it is necessary in the pursuit of a specified operational purpose that has been authorised by the Secretary of State and approved by a Judicial Commissioner. This will apply to both the content of communications and related communications data that may be intercepted under the bulk regime.
K	It is essential that the Agencies can 'discover' unknown threats. This is not just about identifying individuals who are responsible for threats, it is about finding those threats in the first place. Targeted techniques only work on 'known' threats: bulk techniques (which themselves involve a degree of filtering and targeting) are essential if the Agencies are to discover those threats.	The Government welcomes the ISC's acknowledgement of the need to maintain the ability to find those who seek to cause harm to the United Kingdom and our citizens and interests abroad. Part 6 of the draft Bill provides a clear statutory basis for all of the 'bulk' powers used by the agencies for the purpose of discovering previously unknown threats, including the safeguards and oversight arrangements covering the use of these powers.
L	We are satisfied that current legislative arrangements and practice are designed to prevent innocent people's communications being read. Based on that understanding, we acknowledge that GCHQ's bulk interception is a valuable capability that should remain available to them.	The Government is grateful to the ISC for their conclusion that GCHQ's bulk interception capability is a valuable tool and that the current legislative arrangements and practices are designed to prevent innocent people's communications being read. Chapter 1 of Part 6 of the draft Bill carries across all of the existing safeguards that apply to the bulk interception regime. The draft Bill also reduces the number of agencies that can apply for a bulk interception warrant, enhances the authorisation

		regime and limits the purposes for which intercepted communications may be examined
M	While we recognise privacy concerns about bulk interception, we do not subscribe to the point of view that it is acceptable to let some terrorist attacks happen in order to uphold the individual right to privacy – nor do we believe that the vast majority of the British public would. In principle it is right that the intelligence Agencies have this capability, provided – and it is this that is essential – that it is tightly controlled and subject to proper safeguards.	The Government agrees that it is never acceptable to let terrorist attacks happen where they can be prevented. Chapter 1 of Part 6 of the draft Bill ensures the security and intelligence agencies maintain their vital bulk interception capabilities, which will be subject to enhanced safeguards, a more robust authorisation framework and strengthened oversight arrangements.
N	Bulk interception is conducted on external communications, which are defined in law as communications either sent or received outside the UK (i.e. with at least one 'end' of the communication overseas). The collection of external communications is authorised under 19 warrants under Section 8(4) of RIPA. These warrants – which cover the Communications Service Providers who operate the bearers – do not authorise the examination of those communications, only their collection. The warrants are therefore all accompanied by a Certificate which specifies which of the communications collected under the warrant may be examined. GCHQ are not permitted by law to examine the content of everything they collect, only that material which falls under one of the categories listed in the Certificate. In the interests of transparency we consider that the Certificate should be published.	The Government agrees that bulk interception is a vital tool designed to obtain foreign-focussed intelligence. There are strict safeguards governing the use of bulk interception, which ensure the agencies comply fully with their human rights obligations. Applications for bulk interception warrants will continue to be limited to the security and intelligence agencies and only for limited purposes. Proposals in the draft Bill mean that the Certificate will be replaced with a more detailed set of operational purposes for which material intercepted under a bulk warrant may be examined (clauses 107 and 119). Those operational purposes will be authorised in advance by the Secretary of State and approved by a Judicial Commissioner. In circumstances where the intelligence agencies wish to examine a communication of a person known to be in the British Islands they must apply to the Secretary of State for a targeted examination warrant. Publishing the categories of Operational Purposes in detail would be detrimental to national security.
O	8(4) warrants allow GCHQ to collect 'external communications' – these are defined in RIPA as communications where at least one end is overseas. However, in respect of internet communications, the current system of 'internal' and 'external' communications is confusing and lacks transparency. The Government must publish an explanation of which internet communications fall under which category, and ensure that this includes a clear and comprehensive list of communications.	The draft Bill implements the spirit of this recommendation in full; however the Government does not believe that the answer lies in trying to categorise all internet communications according to 'internal' or 'external' criteria. The draft Bill clarifies the current terminology, replacing the definition of 'external' communications with a new requirement that bulk interception warrants should only be authorised where there is a 'foreign focus' – i.e. where the intention is to acquire the communications of persons overseas (clause 106) .

P	The legal safeguards protecting the communications of people in the UK can be summarised as follows: • The collection and examination of communications with both ends known to be in the UK requires an 8(1) warrant. • All other communications can be collected under the authority of an 8(4) warrant. • Of these, GCHQ may search for and select communications to examine on the basis of a selector (e.g. email address) of an individual overseas – provided that their reason for doing so is one or more of the categories described in the 8(4) Certificate. • GCHQ may search for and select communications to examine on the basis of a selector (e.g. email address) of an individual in the UK if – and only if – they first obtain separate additional authorisation from a Secretary of State in the form of an 8(1) warrant or a Section 16(3) modification to the 8(4) warrant. • It would be unlawful for GCHQ to search for communications related to somebody known to be in the UK among those gathered under an 8(4) warrant without first obtaining this additional Ministerial authorisation. • This is reassuring: under an 8(4) warrant the Agencies can examine communications relating to a legitimate overseas target, but they cannot search for the communications of a person known to be in the UK without obtaining specific additional Ministerial authorisation.	The Government thanks the ISC for its helpful summary of the current safeguards that protect the communications of people in the UK. The draft Bill strengthens these further and requires that where an agency seeks to select for examination the communications of a person in the UK it will have to apply to the Secretary of State for a targeted examination warrant, which will need to be approved by a Judicial Commissioner before it can come into force (clause 119).
Q	The nature of the 16(3) modification system is unnecessarily complex and does not provide the same rigour as that provided by an 8(1) warrant. We recommend that despite the additional resources this would require – searching for and examining the communications of a person known to be in the UK should always require a specific warrant, authorised by a Secretary of State.	The Government accepts this recommendation in full. The draft Bill strengthens the safeguards that apply to the communications of persons in the UK, requiring that where an agency seeks to select for examination the communications of a person in the UK it will have to apply to the Secretary of State for a targeted examination warrant, which will need to be approved by a Judicial Commissioner before it can come into force (clause 119).

R	While the protections outlined above apply to people in the UK, they do not apply to UK nationals abroad. While GCHQ operate a further additional system of authorisations, this is a policy process rather than a legal requirement. We consider that the communications of UK nationals should receive the same level of protection under the law, irrespective of where the person is located. The interception and examination of such communications should therefore be authorised through an individual warrant like an 8(1), signed by a Secretary of State. While we recognise this would be an additional burden for the Agencies, the numbers involved are relatively small and we believe it would provide a valuable safeguard for the privacy of UK citizens.	Whilst the Government understands the intention behind the ISC's recommendation it does not believe that there is an objective justification for different protections based purely on nationality. The draft Bill provides strong protections for the examination of content or communications data irrespective of nationality.
S	While the law sets out which communications may be collected, it is the selection of the bearers, the application of simple selectors and initial search criteria, and the complex searches which determine what communications are read. The Interception of Communications Commissioner should be given statutory responsibility to review the various selection criteria used in bulk interception to ensure that these follow directly from the Certificate and valid national security requirements.	The Government agrees that strong oversight of the use of investigatory powers is essential. That is why Part 8 of the draft Bill will reform oversight by creating a new Investigatory Powers Commissioner who will have the power to inspect any aspect of the security and intelligence agencies' use of investigatory powers that he or she considers appropriate, including selection criteria. In addition, a Judicial Commissioner will have a role alongside the Secretary of State in approving the operational purposes for which material collected in bulk can be examined.
T	From the evidence we have seen, there are safeguards in place to ensure that analysts examine material covered by the 8(4) Certificate only where it is lawful, necessary and proportionate to do so. GCHQ's search engines are constructed such that there is a clear audit trail, which may be reviewed both internally and by the Interception of Communications Commissioner. Nevertheless, we were concerned to learn that, while misuse of GCHQ's interception capabilities is unlawful, it is not a specific criminal offence. We strongly recommend that the law should be amended to make abuse of intrusive capabilities (such as interception) a criminal offence.	Unlawful interception is already a criminal offence under the Regulation of Investigatory Powers Act 2000 and clause 2 of the draft Bill replicates this provision. The deliberate misuse of any agency interception capability may also engage existing offences, including misfeasance in public office or offences under the Computer Misuse Act.
U	In our 2013 Report on the draft Communications Data Bill, we concluded that "it is essential that the Agencies maintain the ability to access Communications Data". The Committee remains of that view: it is a critical capability.	The Government shares the Committee's view that it is essential for the Agencies to maintain the ability to access communications data. Part 3 of the draft Bill provides a clear statutory basis for the acquisition of communications data and Part 4 provides for the retention of communications data, both subject to robust safeguards. Chapter 2 of Part 6 makes explicit provision for bulk acquisition of communications

		data and sets out safeguards that apply to related communications data acquired under the bulk interception regime.
V	The Committee considers that the statutory definition of Communications Data – the 'who, when and where' of a communication – is narrowly drawn and therefore, while the volume of Communications Data available has made it possible to build a richer picture of an individual, this remains considerably less intrusive than content. We therefore do not consider that this narrow category of Communications Data requires the same degree of protection as the full content of a communication.	The Government accepts that there is a need to clarify the different types of communications data and accepts the spirit of the ISC's recommendations. Clause 193 of the draft Bill includes revised definitions of the categories of communications data: - Entity data will include data about persons or devices, such as subscriber or billing information. - Event data will include data about interaction between persons or devices, such as the fact of a call between two individuals. Recognising the more intrusive nature of events data, Schedule 4 of the draft Bill requires authorisation of access to such data be at a more senior level than for entity data. In describing the communications data obtained, clause 71 of the draft Bill provides for the retention of internet connection records. The Government recognises the sensitive nature of internet connection records and for that reason clause 47 restricts the purposes for which they can be acquired further than other forms of communications data. A designated senior officer in a public authority will only be able to require disclosure or processing of internet connections records for the following purposes: - To identify the sender of an online communication. This will often be in the form of an IP address resolution and the internet service used must be known in advance of the application - To identify which communication services a person has been using. For example whether they are communicating through apps on their phone - To identify where a person has accessed illegal content. For example an internet service hosting child abuse imagery.
W	However, there are legitimate concerns that certain categories of Communications Data – what we have called 'Communications Data Plus' – have the potential to reveal details about a person's private life (i.e. their habits, preferences and lifestyle) that are more intrusive. This category of information requires greater safeguards than the basic 'who, when and where' of a communication.	

		Clause 71 of the draft Bill also provides that local authorities will not be permitted to acquire internet connection records under any circumstances. Before making a request for communications data, public authorities will need to consider which data type they require access to and whether it is necessary and proportionate to do so.
X	The Agencies' use Bulk Personal Datasets – large databases containing personal information about a wide range of people – to identify individuals in the course of investigations, to establish links, and as a means of verifying information obtained through other sources. These datasets are an increasingly important investigative tool for the Agencies. The Intelligence Services Act 1994 and the Security Service Act 1989 provide the legal authority for the acquisition and use of Bulk Personal Datasets. However, this is implicit rather than explicit. In the interests of transparency, we consider that this capability should be clearly acknowledged and put on a specific statutory footing.	The Government shares the ISC's conclusion that Bulk Personal Datasets are an increasingly important investigative tool for the Agencies. Part 7 of the draft Bill provides explicit statutory safeguards governing the Agencies' acquisition and use of Bulk Personal Datasets. These include a warrantry regime with an authorisation process that is consistent with other bulk capabilities in the draft Bill.
Y	The Intelligence Services Commissioner currently has responsibility for overseeing the Agencies' acquisition, use and destruction of Bulk Personal Datasets. This is currently on a non-statutory basis. Given that this capability may be highly intrusive and impacts upon large numbers of people, it is essential that it is tightly regulated. The Commissioner's role in this regard must therefore be put on a statutory footing.	The government agrees that wherever possible, oversight should be on a statutory basis. That is why, In an immediate response to the ISC's report, the Prime Minister issued a direction to the Intelligence Services Commissioner putting onto a statutory basis his oversight of the Agencies' acquisition, use, retention and destruction of Bulk Personal Datasets. The proposed new Investigatory Powers Commissioner will have a clear remit to oversee the use of all of the powers available to the security and intelligence agencies, including those relating to Bulk Personal Datasets (see clause 169(3)(a)).
CC	The Agencies may undertake IT Operations against computers or networks in order to obtain intelligence. These are currently categorised as 'Interference with Property' and authorised under the same procedure. Given the growth in, and intrusiveness of, such work we believe consideration should be given to creating a specific authorisation regime.	The Government accepts the ISC's recommendation. Part 5 of the Bill provides a bespoke statutory framework for the ability of the Security and Intelligence Agencies, Armed Forces and law enforcement agencies to undertake equipment interference to obtain communications and other private information and imposes strong safeguards that reflect the interception regime (though not in respect of prohibiting the use of product from equipment interference in criminal trials).

FF	In relation to the activities that we have considered thus far, those which are most intrusive are authorised by a Secretary of State. Some witnesses questioned whether Ministers had sufficient time and independence and suggested that the public had lost trust and confidence in elected politicians to make those decisions. The Committee recognises these concerns. However, one aspect which we found compelling is that Ministers are able to take into account the wider context of each warrant application and the risks involved, whereas judges can only decide whether a warrant application is legally compliant. This additional hurdle would be lost if responsibility were to be transferred to judges and may indeed result in more warrant applications being authorised.	The Government shares the ISC's view that it is important that Ministers continue to be able to authorise the use of investigatory powers. The Bill preserves the ability of Ministers to make decisions about the necessity and proportionality of a particular warrant and, in doing so, take account of the wider context and risks involved. The Bill also recognises the need to provide further reassurance that these warrants are subject to robust scrutiny and independent oversight. That is why the draft Bill also includes a new provision for a judicial commissioner to approve warrants before they come into force. The Government feels that this new 'double lock' provides the right balance between the need for executive oversight and accountability and the need to have a robust authorisation process appropriate to the degree of potential intrusion brought about by each type of warrant.
GG	In addition, Ministers are democratically accountable for their decisions. It is therefore right that responsibility for authorising warrants for intrusive activities remains with them. It is Ministers, not judges, who should (and do) justify their decisions to the public. (We consider later the need for greater transparency: the more information the public and Parliament have, the more Ministers will be held to account.)	
HH	Intrusive capabilities which fall below the threshold requiring a warrant are authorised by officials within the relevant Agency or department. While this is appropriate, there should always be a clear line of separation within the Agencies between investigative teams who request approval for a particular activity, and those within the Agency who authorise it. Further, those capabilities that are authorised by officials should be subject to greater retrospective review by the Commissioners to ensure that these capabilities are being authorised appropriately and compensate for the lack of individual Ministerial Authorisation in these areas.	The draft Bill provides that an authorising officer within a public authority may only authorise the acquisition of communications data where they are independent of the relevant operation (clause 47). There is an exemption for national security purposes. The use of these capabilities will be subject to robust independent oversight by the Investigatory Powers Commissioner.

II	The Commissioners' responsibilities have increased as the Agencies' capabilities have developed. However, this has been piecemeal and as a result a number of these responsibilities are currently being carried out on a non-statutory basis. This is unsatisfactory and inappropriate (as the Commissioners themselves recognise). The Commissioners' non-statutory functions must be put on a clear statutory footing.	The Government accepts the need to enhance the already strong oversight regime. Part 8 of the draft Bill creates a new role of Investigatory Powers Commissioner, who will have the ability to inspect and oversee any aspect of the use of investigatory powers that he or she deems appropriate. The Prime Minister will retain the ability to give statutory directions to the Commissioner to inspect or oversee particular aspects of the agencies' work.
JJ	Throughout this Report, we have recommended an increased role for the Commissioners – in particular, where capabilities are authorised at official level. While this would require additional resources, it would mean that the Commissioners could look at a much larger sample of authorisations.	The Government accepts the ISC's recommendation. The Investigatory Powers Commissioner, provided for in Part 8 of the draft Bill, will have a considerable staff, including inspectors and technical experts. The Commissioner will have the ability to draw on independent expert legal advice as necessary.
KK	While oversight systems in other countries include an Inspector General function, we note that Inspectors General often provide more of an internal audit function, operating within the Agencies themselves. As such, the Committee does not accept the case for transferring to this system: it is important to maintain the external audit function that the Commissioners provide.	The Government agrees that it is important to maintain the external audit function that the current Interception of Communications Commissioner, the Intelligence Services Commissioner and the Chief Surveillance Commissioner provide. The draft Bill creates a new office of The Investigatory Powers Commissioner which will provide independent and more visible scrutiny of the agencies and their work (clause 167).
LL	The Investigatory Powers Tribunal is an important component of the accountability structure. However, we recognise the importance of a domestic right of appeal and recommend that this is addressed in any new legislation.	The Government has accepted the ISC's recommendation and the draft Bill provides a domestic route of appeal from the IPT to the Court of Appeal on a point of law (clause 180).
NN	We are reassured that the Human Rights Act 1998 acts as a constraint on all the Agencies' activities. However, this safeguard is not evident to the public since it is not set out explicitly in relation to each intrusive power. The interactions between the different pieces of legislation which relate to the statutory functions of the intelligence and security Agencies are absurdly complicated, and are not easy for the public to understand (we address the requirement for a clearer legal framework later in this chapter).	The Government welcomes the ISC's conclusion that the principles set out in the Human Rights Act 1998 underpin and act as an appropriate constraint all of the activities of the Security and Intelligence Agencies. The draft Bill provides a comprehensive and comprehensible framework governing the acquisition of private communications by the state. All of those powers will be subject to extensive human rights safeguards.

OO	Section 7 of the Intelligence Services Act 1994 allows for a Secretary of State to sign an authorisation which removes civil and criminal liability for activity undertaken outside the British Islands which may otherwise be unlawful under UK law. We have examined the Class Authorisations allowed under ISA in detail and are satisfied that they are required in order to allow the Agencies to conduct essential work. Nevertheless, that may involve intruding into an individual's private life, and consideration should therefore be given to greater transparency around the number and nature of Section 7 Authorisations.	The draft Bill provides a comprehensive basis for all of the powers available to interfere with private communications, including the use of equipment interference to obtain stored communications (currently authorised under the Intelligence Services Act 1994) (provided at Part 5). The Bill does not provide for interference with equipment for purposes other than the acquisition of communications and other private data. All equipment interference under the Bill must be authorised by a warrant, which will require the Agencies to provide details of the operational purposes or a description of the targets of the warrant as appropriate (clauses 81 to 94). The warrants will be renewable every six months.
PP	We consider that Ministers must be given greater detail as to what operations are carried out under each Class Authorisation: a full list should be provided every six months. We also recommend that Ministers provide clear instructions as to what operations they would expect to be specifically consulted on, even if legally no further authorisation would be required.	
QQ	Under the Intelligence Services Act 1994 and Security Service Act 1989, the Agencies are legally authorised to seek intelligence from foreign partners. However, there are currently no legal or regulatory constraints governing how this is achieved.	The Government considers it vital to be able to share intelligence with foreign partners. We work closely with our allies to prevent terrorist attacks and to stop serious and organised criminals from causing harm. Safeguards already exist that govern the sharing of intelligence material. The draft Interception of Communications Code of Practice includes specific details on the sharing of intercept material. The draft Bill creates a new role of Investigatory Powers Commissioner, who will have the ability to inspect and oversee any aspect of the use of investigatory powers that he or she deems appropriate, including arrangements for sharing material with foreign partners.
RR	We have explored in detail the arrangements by which GCHQ obtain raw intercept material from overseas partners. We are satisfied that, as a matter of both policy and practice, GCHQ would only seek such material on individuals whom they themselves are intercepting – therefore there would always be a RIPA warrant in place already.	
SS	We recognise that GCHQ have gone above and beyond what is required in the legislation. Nevertheless, it is unsatisfactory that these arrangements are implemented as a matter of policy and practice only. Future legislation should clearly require the Agencies to have an interception warrant in place before seeking communications from a foreign partner.	

TT	The safeguards that apply to the exchange of raw intercept material with international partners do not necessarily apply to other intelligence exchanges, such as analysed intelligence reports. While the 'gateway' provisions of the Intelligence Services Act and the Security Service Act do allow for this, we consider that future legislation must define this more explicitly and, as set out above, define the powers and constraints governing such exchanges.	
UU	The Committee does not believe that sensitive professions should automatically have immunity when it comes to the interception of communications. However, some specific professions may justify heightened protection. While the Agencies all operate internal safeguards, we consider that statutory protection should be considered (although we acknowledge that it may be difficult to define certain professions).	The Government agrees that it is important that the use of investigatory powers respects the privilege that attaches to certain communications. The draft Bill will not hinder the ability of lawyers and doctors to do their jobs and protect the privacy of their clients and patients. The Bill – and accompanying codes of practice – will provide strong protections for sensitive professions. Codes of practice will underpin all of the powers in the draft Bill and will be required to include provision relating to the safeguards that apply in respect of sensitive professions and privileged material. The draft Bill also makes explicit provision for additional protections in respect of communications to or from certain sensitive professions. Clauses 16 and 85 of the draft Bill introduces a new statutory requirement for a Secretary of State to consult the Prime Minister before issuing a targeted interception warrant, targeted equipment interference warrant or a targeted examination warrant, where it is intended to intercept or examine the communications of a Member of Parliament or other specified legislative member. In addition, the Government recognises that communications data requests intended to identify journalistic sources should attract additional safeguards beyond authorisation at official level. The Communications Data Code of Practice currently requires public authorities to seek judicial authorisation before obtaining communications data to identify a journalistic source. Clause 61 of the draft Bill puts this requirement onto a statutory footing.

VV	Given the nature of current threats to the UK, the use of Directions under the Telecommunications Act is a legitimate capability for the Agencies. However, the current arrangements in the Telecommunications Act 1984 lack clarity and transparency, and must be reformed. This capability must be clearly set out in law, including the safeguards governing its use and statutory oversight arrangements.	The Government accepts the ISC's conclusion and has included provisions in Part 6 of the draft Bill for the acquisition of communications data in bulk, to put this capability on a more transparent footing, with strengthened safeguards. Strict safeguards are already in place, including regular Secretary of State review of whether the capability continues to be necessary and proportionate. For more than 10 years, successive governments have authorised this critical capability. In a similar way to warrants, Secretaries of States authorise the continued use of Directions on a 6 monthly basis and they are overseen by the Intelligence Services Commissioner. The capability has provided fast and secure access to communications data so that the Agencies can join the dots in their investigations. The draft Bill strengthens these safeguards even further. The power will become subject to the 'double-lock' safeguard of Ministerial and Judicial authorisation and the data is only accessible for specified Operational Purposes. A bulk communications data warrant will have to meet the following test: there must be a national security justification for acquiring the data, it must be necessary and proportionate, and both a Secretary of State and a Judicial Commissioner must approve it. Warrants will last for six months, subject to renewal. Access to data on a day-to-day basis will be strictly controlled and subject to internal justification on grounds of necessity and proportionality. The new Investigatory Powers Commissioner – a senior judge – will provide oversight of the use of this capability. Clause 188 of the Bill provides a power for the Secretary of State to issue a national security notice requiring an operator to take necessary steps in the interest of national security. The type of support that may be required includes the provision of services or facilities which would help the intelligence agencies in safeguarding the security of their personnel and operations, or in providing assistance with an emergency (as defined in the Civil Contingencies Act 2004). The Bill makes clear that a national security notice cannot be used for the primary purpose of interfering with privacy, obtaining communications or data. In any circumstance where a notice would involve interference with privacy or the acquisition of communications or data as its main aim, an

		additional warrant or authorisation provided for elsewhere in the Bill would always be required. As such, a notice of itself does not authorise an intrusion into an individual's privacy.
WW	While our previous recommendations relate to the changes that would be required to the existing legislative framework, the evidence that we have seen suggests that a more fundamental review is now overdue.	The introduction of the draft Bill illustrates the Governments acceptance of the ISC's recommendation. The draft Bill provides a comprehensive and comprehensible framework governing the acquisition of private communications by the state.

YY	The new legislation should clearly list each intrusive capability available to the Agencies (including those powers which are currently authorised under the implicit authorities contained in the Intelligence Services Act and the Security Service Act) and, for each, specify: a. The purposes for which the intrusive power can be used (one or more of: the protection of national security, the safeguarding of the economic well-being of the UK, or the detection or prevention of serious crime). b. The overarching human rights obligations which constrain its use. c. Whether the capability may be used in pursuit of a specific person, location or target, or in relation to a wider search to discover unknown threats. d. The authorisation procedures that must be followed, including the review, inspection and oversight regime. e. Specific safeguards for certain individuals or categories of information – for example, UK nationals, legally privileged information, medical information etc. (This should include incidental collection where it could not reasonably have been foreseen that these categories of information or individuals might be affected.) f. Retention periods, storage and destruction arrangements for any information obtained. g. The circumstances (including the constraints that might apply) in which any intelligence obtained from that capability may be shared with intelligence, law enforcement or other bodies in the UK, or with overseas partners. h. The offence which would be committed by Agency personnel abusing that capability. i. The transparency and reporting requirements.	The Government acknowledges the need to ensure that the public are able to understand the laws governing when and how the security and intelligence agencies and law enforcement are allowed to obtain and use their information. The draft Bill provides a clear and comprehensible framework that clarifies which powers different agencies can use and for what purpose. It specifies: - The purposes for which each power may be used and the statutory tests that must be satisfied before a power can be used. - The safeguards that apply to each of the powers, including consideration of wider human rights obligations. - Whether powers must be directed at an individual or a specific operation, or whether they may be used to acquire data in bulk for target discovery purposes. - The authorisations process that applies to each power, reflecting the sensitivity and intrusiveness of that power. - The Codes of Practice that must be laid in respect of each power and which will set out specific safeguards for sensitive professions and privileged material. - The retention, storage and destruction safeguards that apply to material obtained under each of the powers, including, where appropriate, provision through Codes of Practice. - The offences that will apply to unauthorised use of powers and capabilities, including the offence of unlawful interception and wilful and reckless acquisition of communications data without lawful authority. - The role of the Investigatory Powers Commissioner in overseeing the use of those powers and ensuring appropriate levels of transparency to aid public understanding.

ZZ	In terms of the authorisation procedure, the following principles should apply: a. The most intrusive activities must always be authorised by a Secretary of State. b. When considering whether to authorise the activity, the Secretary of State must take into account, first, legal compliance and, if this is met, then the wider public interest. c. All authorisations must include a summary of the expected collateral intrusion, including an estimate of the numbers of innocent people who may be impacted, and the extent to which the privacy of those innocent people will be intruded upon. d. Any capability or operation which would result in significant collateral intrusion must be authorised by a Secretary of State. e. All authorisations must be time limited (usually for no longer than six months). f. Where an authorisation covers classes of activity conducted overseas, this must include the requirements for recording individual operations conducted under those authorisations, and the criteria for seeking separate Ministerial approval. g. Where intelligence is sought from overseas partners, the same authorisation must be obtained as if the intrusive activity was undertaken by the UK Agency itself. h. Where unsolicited material is received, the circumstances in which it may be temporarily held and assessed, and the arrangements for obtaining retrospective authority (or where authority is not given, destruction of the material) must be explicitly defined.	The draft Bill provides for enhanced authorisation arrangements, including: - Strict legal tests that must be satisfied before authorising a particular activity or imposing an obligation on a communications service provider. - A requirement to take into account collateral intrusion arising as a result of a particular interference. - A strict time limit on each authorisation (ordinarily six months, subject to renewal or review)

AAA	In relation to communications, given the controversy and confusion around access to Communications Data, we believe that the legislation should clearly define the following terms: - 'Communications Data' should be restricted to basic information about a communication, rather than data which would reveal a person's habits, preferences or lifestyle choices. This should be limited to basic information such as identifiers (email address, telephone number, username, IP address), dates, times, approximate location, and subscriber information. - 'Communications Data Plus' would include a more detailed class of information which could reveal private information about a person's habits, preferences or lifestyle choices, such as websites visited. Such data is more intrusive and therefore should attract greater safeguards. - 'Content-Derived Information' would include all information which the Agencies are able to generate from a communication by analysing or processing the content. This would continue to be treated as content in the legislation.	The draft Bill includes revised definitions of the categories of communications data (clause 193): - Entity data will include data about persons or devices, such as subscriber or billing information. - Event data will include data about interaction between persons or devices, such as the fact of a call between two individuals. Before making a request for communications data, public authorities will need to consider which data type they require access to and whether it is necessary and proportionate to do so. Due to the potentially higher level of intrusion associated with Event data, its acquisition must be authorised at a more senior level within the police or other public authorities. Separate safeguards will apply to the acquisition of Related Communications Data (including that derived from content) which may be obtained as a result of bulk interception.
BBB	The Committee has identified a number of areas where we believe there is scope for the Government to be more transparent about the work of the Agencies. The first step – as previously set out – is to consolidate the relevant legislation and avow all of the Agencies' intrusive capabilities. This will, in itself, be a significant step towards greater transparency. Where it is not practicable to specify the detail of certain arrangements in legislation, the Government must nevertheless publish information as to how these arrangements will work (for example, in Codes of Practice). We recognise that much of the detail regarding the Agencies' capabilities must be kept secret. There is, however, a great deal that can be discussed publicly and we believe that the time has come for much greater openness and transparency regarding the Agencies' work.	This draft Bill provides more detail than ever before about the powers available to the agencies, how they are authorised, and the safeguards that apply to them. It will be underpinned by detailed statutory codes of practice. The Investigatory Powers Commissioner will play a visible, independent role in overseeing the work of the agencies and ensuring there is appropriate transparency and public understanding of how they work.