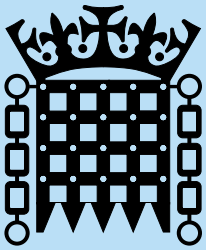

Intelligence and Security Committee of Parliament

Report on the draft Investigatory Powers Bill

Chair:
The Rt. Hon. Dominic Grieve QC MP

Intelligence and Security Committee of Parliament

Report on the draft Investigatory Powers Bill

Chair:
The Rt. Hon. Dominic Grieve QC MP

Presented to Parliament pursuant to Section 3 of the Justice and Security Act 2013

Ordered by the House of Commons to be printed on 9 February 2016

HC 795

This publication is available at www.gov.uk/government/publications

Any enquiries regarding this publication should be sent to us via isc.independent.gov.uk/contact

Print ISBN 9781474127714
Web ISBN 9781474127721

ID 26011601 02/16 53894 19585

Printed on paper containing 75% recycled fibre content minimum

Printed in the UK by the Williams Lea Group on behalf of the Controller of Her Majesty's Stationery Office

THE INTELLIGENCE AND SECURITY COMMITTEE OF PARLIAMENT

The Intelligence and Security Committee of Parliament (ISC) is a statutory committee of Parliament that has responsibility for oversight of the UK intelligence community. The Committee was originally established by the Intelligence Services Act 1994, and has recently been reformed, and its powers reinforced, by the Justice and Security Act 2013.

The Committee oversees the intelligence and security activities of the UK, including the policies, expenditure, administration and operations[1] of the Security Service (MI5), the Secret Intelligence Service (SIS) and the Government Communications Headquarters (GCHQ). The Committee also scrutinises the work of other parts of the UK intelligence community, including the Joint Intelligence Organisation and the National Security Secretariat in the Cabinet Office; Defence Intelligence in the Ministry of Defence; and the Office for Security and Counter-Terrorism in the Home Office.

The Committee consists of nine Members drawn from both Houses of Parliament. The Chair is elected by its Members. The Members of the Committee are subject to Section 1(1)(b) of the Official Secrets Act 1989 and are routinely given access to highly classified material in carrying out their duties.

The Committee sets its own agenda and work programme. It takes evidence from Government Ministers, the heads of the intelligence Agencies, officials from the intelligence community, and other witnesses as required. The Committee is supported in its work by an independent Secretariat and an Investigator. It also has access to legal, technical and financial expertise where necessary.

The Committee produces an Annual Report on the discharge of its functions. The Committee may also produce Reports on specific investigations. Prior to the Committee publishing its Reports, sensitive material that would damage national security is blanked out ('redacted'). If required, this is indicated by *** in the text. The intelligence and security Agencies may request the redaction of material in the Report if its publication would damage their work, for example by revealing their targets, methods, sources or operational capabilities. The Committee considers these requests for redaction carefully. The Agencies have to demonstrate clearly how publication of the material in question would be damaging before the Committee agrees to redact it. The Committee aims to ensure that only the minimum of text is redacted from the Report. The Committee believes that it is important that Parliament and the public should be able to see where information had to be redacted. This means that the published Report is the same as the classified version sent to the Prime Minister (albeit with redactions). The Committee also prepares from time to time wholly confidential reports which it submits to the Prime Minister.

[1] *Subject to the criteria set out in Section 2 of the Justice and Security Act 2013.*

INTRODUCTION

1. The UK intelligence and security Agencies – the Security Service (MI5), the Secret Intelligence Service (SIS) and the Government Communications Headquarters (GCHQ) – exist to protect the national security of the country. In order to do so, they employ certain intrusive capabilities to collect information covertly, both in the UK and overseas. There has been considerable debate over the past few years regarding both the necessity and extent of those capabilities – particularly given the considerable changes in technology since the laws authorising the Agencies to use these powers were passed.

2. In March 2015, the Intelligence and Security Committee of Parliament (ISC) published *Privacy and Security: A modern and transparent legal framework*. This was a detailed investigation into the intrusive capabilities used by the Agencies. The Committee concluded that the investigatory powers the Agencies were authorised to employ were necessary and proportionate – and we remain of this view. However, the Committee did not consider that there was sufficient openness or transparency about those powers. Our key recommendation therefore was that the current legal framework governing the Agencies' powers should be replaced by a new Act of Parliament, clearly setting out all the intrusive powers available to the Agencies, the purposes for which they may use them, and the authorisation required before they may do so. We considered this an essential step in seeking to protect both security and privacy.

3. In November 2015, the Government published the draft Investigatory Powers Bill ('the draft Bill'), in response to a number of independent reviews such as the one by this Committee. In late November 2015, a Joint Committee of Parliament was appointed to undertake pre-legislative scrutiny of the draft Bill. However, given the role of the ISC in overseeing the intelligence and security Agencies, and its ability to take evidence on classified matters, this Committee has provided scrutiny of those aspects of the draft Bill which relate to the Agencies' investigatory powers. There are, of course, a number of other important policy issues in the draft Bill (for instance, the 'double-lock' authorisation) on which the Committee has chosen not to comment in this Report, since they rightfully fall to the Joint Committee. We are grateful to the Chairman of the Joint Committee, Lord Murphy of Torfaen, for his help in ensuring that the two Committees were able to work together successfully.

4. The draft Bill makes some attempt to improve transparency; however, the Committee is disappointed to note that it does not cover all the Agencies' intrusive capabilities. This failure to address the Committee's key recommendation means that various powers and authorisations remain scattered throughout different pieces of legislation. As a result, the draft Bill is handicapped from the outset in terms of the extent to which it can provide a clear and comprehensive legal framework to govern the use and oversight of investigatory powers. This is – in our view – a significant missed opportunity.

5. Nevertheless, we have considered the draft Bill insofar as it goes, and in this Report we have outlined the issues that we believe are cause for concern:

   i. Overall, the privacy protections are inconsistent and in our view need strengthening. We recommend that an additional Part be included in the new legislation to provide universal privacy protections, not just those that apply to sensitive professions.

ii. The provisions in relation to three of the key Agency capabilities – Equipment Interference, Bulk Personal Datasets and Communications Data – are too broad and lack sufficient clarity.

iii. In addition to these major issues of principle, there are a number of more detailed matters requiring specific amendments. These can be found at the end of this Report.

6. The Investigatory Powers Bill is the first major piece of legislation governing the Agencies' powers in over 15 years. While the issues under consideration are undoubtedly complex, we are nevertheless concerned that thus far the Government has missed the opportunity to provide the clarity and assurance which is badly needed. That the confusion surrounding the existing legislation fuelled many of the allegations and suspicions concerning the Agencies' investigatory powers over the past few years clearly demonstrates the importance of transparency in this area.

7. The issues we have highlighted in this Report must be addressed before any subsequent Bill is laid before the House and we would urge the Government to ensure that it takes sufficient time and care in so doing. While we recognise the timing constraints imposed by the 'sunset clause' in the Data Retention and Investigatory Powers Act 2014, it appears that the draft Bill has perhaps suffered from a lack of sufficient time and preparation and it is important that this lesson is learned prior to introduction of the new legislation.

KEY AREAS OF CONCERN

Privacy protections

8. Given the background to the draft Bill and the public concern over the allegations made by Edward Snowden in 2013, it is surprising that the protection of people's privacy – which is enshrined in other legislation – does not feature more prominently. One might have expected an overarching statement at the forefront of the legislation, or to find universal privacy protections applied consistently throughout the draft Bill. However, instead, the reader has to search and analyse each investigatory power individually to understand the privacy protections which may apply. This results in a lack of clarity which undermines the importance of the safeguards associated with these powers.

9. It is the view of this Committee that privacy protections should form the backbone of the draft legislation, around which the exceptional powers are then built. Whilst recent terrorist attacks have shown the importance of the work the Agencies do in protecting us, this cannot be used as an excuse to ignore such important underlying principles or unnecessarily override them. Privacy considerations must form an integral part of the legislation, not merely an add-on.

10. This approach should also be applied to the additional protections afforded to certain sensitive professions. However, again, these are mentioned sporadically throughout and do not appear to be applied consistently. For example, Clause 61 sets out that a Judicial Commissioner must approve an authorisation to obtain Communications Data for the purpose of identifying a source of journalistic information. However, this clause does not apply to the Agencies. A further example is the protection afforded to a *"member of a relevant legislature"*: whilst the Secretary of State is required to consult the Prime Minister before issuing a Targeted Interception, Targeted Examination or Targeted Equipment Interference warrant where the communications are sent by, or intended for, a person who is a *"member of a relevant legislature"*, similar protections are not provided for in relation to Bulk Personal Dataset or Bulk Acquisition warrants.

A. The new legislation should include a single additional Part that addresses privacy safeguards and clearly sets out universal privacy protections which apply across the full range of investigatory powers.

B. Where additional protection is provided for sensitive professions, these safeguards must be applied consistently, no matter which investigatory power is used to obtain the information. The new legislation should be amended to rectify this inconsistency.

Equipment Interference

- ➢ The Agencies undertake Equipment Interference (EI) against computers or networks, both within the UK and overseas. Such activity is currently categorised as 'Interference with Property' and is authorised by a warrant under the Intelligence Services Act 1994.
- ➢ The draft Bill provides for a new, explicit EI regime. Clauses 81–105 cover Targeted Equipment Interference warrants and Clauses 135–149 cover Bulk Equipment Interference warrants.
- ➢ The Committee has three primary concerns with how EI is authorised under the draft Bill:
  - i. EI where the primary purpose is not to obtain information;
  - ii. the requirement for Bulk EI warrants; and
  - iii. EI conducted overseas.

11. The draft Bill authorises the Agencies to conduct Equipment Interference (EI) to obtain information ('Computer Network Exploitation'). However, the Agencies also conduct several different forms of EI that are not provided for under the draft Bill. These IT operations will continue to sit under the broad authorisations provided to the Agencies under the Intelligence Services Act 1994.

12. This discrepancy as to how similar activity will be authorised appears inconsistent with the Government's aim of simplifying the legislation underpinning the Agencies' intrusive powers. It means that certain IT operations will require a different standard of authorisation (without Judicial Commissioner approval) than Computer Network Exploitation and that similar activities undertaken by the Agencies will be authorised under different pieces of legislation.

13. In addition, retaining certain IT operations under the broad 'property interference' provisions of the Intelligence Services Act 1994 fails to achieve transparency in this area and effectively means that such operations remain 'secret' and thus not subject to clear safeguards.

C. The Committee recommends that all IT operations are brought under the provisions of the new legislation. This will ensure that all types of Equipment Interference are governed under the same legislation, with the same authorisation process and the same safeguards.

14. As set out above, the draft Bill provides for Targeted and Bulk EI warrants. However, despite the name, a Targeted EI warrant is not limited to an individual piece of equipment, but can relate to all equipment where there is a common link between multiple people, locations or organisations. In evidence, the Director of GCHQ suggested that, hypothetically, a Targeted EI warrant could cover a target as broad as an entire hostile foreign intelligence service. It is therefore unclear what a 'Bulk' EI warrant is intended to cover, and how it differs from a 'Targeted' EI warrant – a concern recognised by the

Director of GCHQ who noted that *"the dividing line between a large-scale targeted EI and bulk is not an exact one"*.[2]

15. The Agencies appeared to suggest that the provision of a Bulk EI warrant is necessary for 'future-proofing', but they could not provide any specific examples as to what these warrants might cover. The Committee is therefore not convinced as to the requirement for them.

D. The Committee acknowledges that the Agencies need the capability to undertake Equipment Interference as necessary. However, the Committee has not been provided with sufficiently compelling evidence as to why the Agencies require Bulk Equipment Interference warrants, given how broadly Targeted Equipment Interference warrants can be drawn. The Committee therefore recommends that Bulk Equipment Interference warrants are removed from the new legislation.

16. A further concern with Targeted EI warrants is that they are only mandatory for Computer Network Exploitation operations in the UK: they are 'optional' for overseas operations. (This is to cover, for example, agents working in hostile environments who often need to exploit opportunities as soon as they become available, rather than applying for a warrant first.) Providing the Agencies with the 'option' of obtaining an authorisation is a curious approach: why would they apply for a warrant if they are not required to do so? If this new legislation is intended to provide certainty and assurance, then this is one aspect which must be clarified.

E. The Committee recommends 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.

[2] *Oral evidence – Tri-Agency, 26 November 2015.*

Bulk Personal Datasets

- Bulk Personal Datasets (BPDs) are large datasets containing personal information about a wide range of people. The Agencies use these datasets in three ways:
  i. to help identify Subjects of Interest, or unknown individuals who surface in the course of investigations;
  ii. to establish links between individuals and groups, or else improve understanding of a target's behaviour and connections; and
  iii. as a means of verifying information that was obtained through other sources (such as agents).
- The Committee examined the Agencies' use of BPDs in its *Privacy and Security* Report and concluded that *"these datasets are an increasingly important investigative tool for the Agencies"*.[2] Examples of BPDs include passport application data, telephone directories and electoral rolls.
- BPDs are provided for in Clauses 150–166 of the draft Bill. The Committee has two primary concerns as to how this capability is authorised under the draft Bill:
  i. the use of Class BPD warrants; and
  ii. the temporary retention of BPDs.

17. The draft Bill provides for two new types of warrant to obtain, retain and examine Bulk Personal Datasets (BPDs) – Specific BPD warrants and Class BPD warrants. In the case of Specific BPD warrants, the Agencies must seek Ministerial and judicial authorisation for each individual dataset; however, a Class BPD warrant allows the Agencies to obtain any number of datasets falling within a category (e.g. travel data) without specifically informing Ministers of each one. This therefore means that a number of BPDs can be obtained without any specific Ministerial consideration of the intrusion into privacy involved in relation to each individual dataset. The Agencies have told the Committee that they anticipate that the majority of BPD warrants will be class based.

18. As a matter of principle, the Committee considers that class authorisations should be kept to an absolute minimum and subject to greater safeguards, as we set out in our *Privacy and Security* Report. We have explored with the Agencies why class warrants are thought to be important in relation to BPDs. The sole factor appears to be the practical impact due to the very significant increase in warrant applications if they were required to obtain a warrant for every individual BPD. We are mindful of the pressures on the Agencies and would not seek to add to their administrative workload without good reason.[4] However, BPDs contain personal information about a large number of individuals, the majority of whom will not be of any interest to the Agencies. Given the volume of the material concerned, and the number of individuals covered, the Committee does not feel that such practical considerations are sufficient to override privacy concerns. In the context of BPDs, provision for class warrants risks over-reliance on them and undermines the safeguards and protections in place for acquiring individual datasets.

---

[3] *Privacy and Security: A modern and transparent legal framework, Intelligence and Security Committee of Parliament, March 2015, page 59.*

[4] *This increase in workload would also apply to Ministers. However, we note that this might be mitigated by limiting Ministerial authorisation to the initial acquisition of datasets, with retention and ongoing use then authorised solely by a Judicial Commissioner.*

F. The Committee considers 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.

19. There is a further issue concerning BPDs, which relates to the provision the draft Bill makes for the Agencies to hold (but not use) a dataset temporarily whilst they apply for the necessary warrant. Having explored the rationale for this exception with the Agencies, we understand that it is to allow for circumstances when the data may be obtained opportunistically. Whilst we recognise the need for such a circumstance to be covered, we are nevertheless concerned that the draft Bill does not impose any time limit by which the warrant application must be made. In theory, therefore, an Agency could hold a BPD without authorisation indefinitely. This clearly is not appropriate. Indeed, when asked whether there was any reason why there should not be a time limit on the face of the Bill, the Director General of MI5 said *"I can't see what our principal objection would be"*.[5]

G. Whilst it is reasonable to allow the Agencies a period of grace in which to apply for a Specific Bulk Personal Dataset warrant where a Bulk Personal Dataset has been obtained opportunistically, that period should be specified on the face of the new legislation to ensure that no Bulk Personal Dataset can be held without authorisation for an undue length of time. The Committee recommends that a time limit of one month is introduced for the Agencies to hold a UK-sourced Bulk Personal Dataset without a warrant temporarily whilst a specific warrant application is made and determined. In the case of overseas-sourced Bulk Personal Datasets, this time limit should be six months.

[5] *Oral evidence – Tri-Agency, 26 November 2015.*

Communications Data

- ➢ Communications Data means the details about a communication (the 'who, when and where') but not the content of what was said or written.
- ➢ Communications Data is central to most Agency investigations. It is used to develop intelligence leads, to help focus on individuals who may pose a threat to the UK, to ensure that interception is properly targeted and to illuminate networks and associations relatively quickly.
- ➢ The Committee has identified two primary concerns in the draft Bill in relation to Communications Data:
  - i. inconsistent processes and safeguards for the examination of Communications Data; and
  - ii. the transparency of the arrangements relating to how the Agencies obtain Internet Connection Records (ICRs).

20. The Agencies have several different mechanisms for obtaining Communications Data, including:

i. individual requests to Communication Service Providers (CSPs) (Clauses 46–70 in the draft Bill);

ii. Bulk Acquisition of Communications Data from CSPs (Clauses 122–134 in the draft Bill);

iii. Related Communications Data (RCD) from Bulk Interception (Clauses 106–121 in the draft Bill); and

iv. requests from overseas partners (authorised under the 'gateway' provisions of the Intelligence Services Act 1994 and Security Service Act 1989).

21. However, these different methods are not authorised in a consistent manner in the draft Bill: as a result, there are a variety of different safeguards and authorisation procedures for obtaining and examining the same information. This is a missed opportunity to clarify procedures and provide the *"enhanced, consistent safeguards"*[6] that the new legislation is intended to provide.

22. For example, if an MI5 officer wishes to make a direct request to a CSP for Communications Data, this request (which must be necessary and proportionate, and for at least one of the ten specified purposes listed in the draft Bill) would be submitted to a Designated Senior Officer for authorisation. In contrast, where Communications Data is being examined under a Bulk Acquisition warrant, the draft Bill contains less detailed provisions as to how an MI5 officer is to obtain authorisation. Whilst the Agencies may choose to apply the same processes in both circumstances as a matter of policy and good practice, this is not required by the draft Bill.

[6] *Foreword from the Home Secretary, Draft Investigatory Powers Bill, November 2015.*

23. A further example is in relation to GCHQ's collection of RCD via its Bulk Interception capabilities. RCD encompasses all aspects of the communication apart from the actual content. GCHQ does not seek to collect the communications of people in the UK, but some incidental interception is inevitable because the origin of the sender or recipient is not always clear – for example, an email address ending '.com' could belong to a person in the UK. To provide protection for any such material incidentally collected, there is a prohibition on searching for and examining any material that relates to a person known to be in the UK (therefore, even if it is collected, it cannot be examined unless additional authorisation is obtained). However, these safeguards only relate to the content of these communications. The RCD relating to the communications of people in the UK is unprotected if it is collected via Bulk Interception. In direct contrast, if the same material were collected and examined through other means (for example, a direct request to a CSP) then the draft Bill sets out how it must be authorised (i.e. through a Designated Senior Officer). Again, the Agencies may choose to apply the same processes in both circumstances as a matter of policy and good practice, but this is not required by the draft Bill. To leave the safeguards up to the Agencies as a matter of good practice is simply unacceptable: this new legislation is an opportunity to provide clarity and assurance and it fails to do so in this regard.

H. The approach towards the examination of Communications Data in the draft Bill is inconsistent and largely incomprehensible. The Committee recommends that the same process for authorising the examination of any Communications Data (including Related Communications Data) is applied, irrespective of how the Agencies have acquired the data in the first instance. This must be clearly set out on the face of the Bill: it is not sufficient to rely on internal policies or Codes of Practice.

24. The draft Bill also introduces a new power for law enforcement organisations and the Agencies to acquire Internet Connection Records (ICRs). The Agencies have told the Committee that, given that they have a range of other capabilities which enable them to obtain equivalent data (and the fact that they do not have the same requirements for evidential material as law enforcement), the power to obtain ICRs set out in Part 3 of the draft Bill will be used primarily by law enforcement organisations. The draft Bill is not clear on this issue, resulting in a lack of transparency.

I. The draft Bill provides for access to Internet Connection Records through a specific request to a Communications Service Provider under Part 3. This could be interpreted as being the only way in which Internet Connection Records may be obtained. However, this is misleading: the Agencies have told the Committee that they have a range of other capabilities which enable them to obtain equivalent data. In the interests of transparency, the draft Bill should be amended to make this clearer.

---

25. The changes we have highlighted above will ensure that a more consistent and comprehensible Bill can be introduced to Parliament which will both maintain the Agencies' vital capabilities and also strengthen the safeguards and controls governing their use. In addition to these major issues of principle, we have set out in the next section a number of more detailed and specific amendments required.

FURTHER SPECIFIC AMENDMENTS REQUIRED

J. There are a number of other aspects of the draft Bill which the Committee considers require amendment. We have listed these below.

i. A Secretary of State may issue a Targeted Interception warrant if it is necessary for (a) national security; (b) preventing or detecting serious organised crime; or (c) economic well-being so far as is relevant to national security and relates to people outside the British Islands. This is unnecessarily confusing and complicated: if 'national security' is sufficient in itself, then *"economic well-being… so far as [is] relevant to the interests of national security"* is redundant, since it is a subset of the former. We have questioned both the Agencies and the Home Office on this matter and neither have provided any sensible explanation. In our opinion, this area is already sufficiently complex so drafters should seek to minimise confusion wherever possible. We therefore recommend that 'economic well-being' is removed as a separate category.

ii. The draft Bill provides that all Bulk warrants must specify the 'operational purpose' for which the material collected is being examined; however, no detail is provided as to what these operational purposes may be. The Committee considers this completely unsatisfactory: it contradicts the primary purpose of the draft Bill, to provide some much-needed transparency in this area. The Committee therefore recommends that some detail on the 'specified operational purposes' for which material obtained under a Bulk warrant can be examined should be published – only then can Parliament properly evaluate the provisions of the new legislation in this area.

    We recognise, however, that it may not be possible to publish full details of the specified operational purposes. In such circumstances, this Committee would expect to be able to examine the secret material on behalf of Parliament, and to provide assurances or recommendations, as appropriate, to our parliamentary colleagues and to the public. However, the Committee has been told that the list of operational purposes has not yet been finalised by Government, and that it will not be finalised until after the Bill itself has been passed. The Committee is therefore unable to provide any reassurance that these 'operational purposes' are appropriate. We fail to see how Parliament is expected to approve any legislation when a key component, on which much of it rests, has not been agreed, let alone scrutinised by an independent body.

iii. The draft Bill provides that, where the communications of a person known to be in the UK have been obtained via Bulk Interception or Bulk Equipment Interference, the Agencies require a Targeted Examination warrant before they can examine it. The draft Bill appears to suggest that Targeted Interception and Targeted Examination warrants are very similar. For the sake of clarity, further thought should therefore be given to creating a single warrant covering the content of the communications of a person in the UK, thereby ensuring that the same safeguards and authorisation procedures apply, irrespective of the way in which the material was obtained.

iv. Where GCHQ has collected UK material through Bulk Interception, the draft Bill allows a 'grace period' of five working days during which GCHQ

can continue to examine the material without a specific warrant (solely with the authorisation of a senior official). This is the only scenario in which interception of a person known to be in the UK may take place without a warrant: it is therefore essential that additional safeguards are included in the new legislation – for example, through mandatory retrospective scrutiny by the Judicial Commissioners.

v. We have similar concerns regarding the timeframes in respect of 'urgent' warrants. The draft Bill allows for a five working day 'grace period' in circumstances where the Agencies consider that a warrant is required urgently: in these circumstances, the Secretary of State may issue the warrant before the Judicial Commissioner has approved it. While we recognise the need for a procedure to handle urgent cases, five working days is unnecessarily long. The Committee recommends that the maximum period for which a warrant may be operational without judicial authorisation is two working days.

vi. While the draft Bill contains some much-needed reforms of the current Commissioners which should increase the current limited oversight, there is one further addition which the Committee considers necessary. At present, when this Committee is informed of matters that would more appropriately fall to the Commissioners or the Investigatory Powers Tribunal, there is no mechanism through which these can be formally referred to them for investigation. It would therefore be sensible for this Committee – on behalf of Parliament – to be given such a power.

vii. In the Committee's Report on *Privacy and Security*, we recommended that 'thematic' Targeted Interception warrants be used sparingly and subject to greater safeguards; unfortunately this has not been reflected in the draft Bill. The Committee reiterates its earlier recommendation: as a minimum, 'thematic' warrants should be authorised for a shorter time period (one month, as opposed to the usual six) to ensure that they receive the greater scrutiny required.

viii. The Committee recommended previously that there should always be a clear line of separation between investigative teams who request approval for a particular activity and those within the Agency who authorise it. The draft Bill requires this division when obtaining Communications Data but the Agencies are exempt from this requirement. Whilst we have been told that this would create an unnecessary burden and time delay, given how regularly the Agencies use Communications Data, we nevertheless consider separation an important matter of principle and recommend that this is reconsidered before legislation is brought forward.

ix. Clause 164 of the draft Bill states that when a Class BPD warrant is not renewed, or is cancelled, the Secretary of State may (with the approval of a Judicial Commissioner) authorise the retention or examination of any of the material. This appears to circumvent the warrantry process: if the Agencies wish to retain and use information contained within a BPD, they should seek a new warrant. The Committee recommends that, in circumstances where a Class BPD warrant is not renewed, or is cancelled, and the Agencies wish to continue retaining or examining any of the material, a new Specific BPD warrant must be sought. The Committee therefore recommends that the Government amend this clause accordingly.

x. The draft Bill imposes several obligations on CSPs to assist the Agencies. For example, Clause 189 states that the Secretary of State may make *"technical capability"* regulations. Some CSPs have expressed serious concern as to this seemingly open-ended and unconstrained power, suggesting that this may lead to banning end-to-end encryption. The Home Office must ensure that the legislation provides clarity as to the nature and scale of these obligations.

xi. A key issue arising from the Committee's *Report on the intelligence relating to the murder of Fusilier Lee Rigby* was the difficulties the Agencies face in accessing communications content from CSPs based overseas. Whilst the draft Bill asserts extraterritoriality, the Agencies have told the Committee that additional measures are needed, and that the CSPs themselves are pressing for an international framework to be developed. Although some initial discussions have taken place, the Committee is disappointed that the Government has not done more to make progress on this crucial issue, and we reiterate our earlier recommendation that this matter must be resolved urgently; without proper progress, the Agencies' hands are tied.

xii. The statutory basis for the Agencies' exchange of material with international partners will continue to sit under general authorisations in the Security Service Act 1989 and the Intelligence Services Act 1994.[7] The draft Bill does not, therefore, meet the recommendations made in the Committee's *Privacy and Security* Report that future legislation must set out these arrangements more explicitly, defining the powers and constraints governing such exchanges. The Committee recommends that the new legislation is amended to reflect this recommendation: the proportion of intercept material obtained from international partners is such that it is not appropriate to exclude it from legislation which purports to cover interception.

xiii. The Mutual Assistance warrant regime in the draft Bill seeks to replicate the infrequently used provisions in the Regulation of Investigatory Powers Act 2000 (RIPA) governing interception undertaken under Mutual Legal Assistance Treaties. The Committee considers that these warrants have been given greater prominence in the draft Bill than they deserve which may give a misleading impression as to their nature. We recommend this should be clarified.

Clause 39 of the draft Bill seeks to replicate existing provisions in RIPA which give effect to the EU's Convention on Mutual Assistance in Criminal Matters, allowing interception in the UK to be conducted on behalf of a foreign partner. However, it omits the restriction in RIPA that the person being intercepted must be outside the UK. This therefore would allow for UK residents to be intercepted in the UK without a warrant being in place. Given that the Committee has not been given a reason for this omission, we presume this is a drafting error: in our view it is essential that the original RIPA safeguard is reinstated, and the communications of those in the UK properly protected.

[7] *The draft Bill does, however, subject these general authorisations to certain safeguards, for example Clauses 40 and 41 with regard to Targeted Interception and Clauses 117 and 118 with regard to Bulk Interception. Additionally, paragraph 2 of Schedule 6 requires a Code of Practice to cover the issue of exchange with overseas partners.*

ANNEX: LIST OF WITNESSES

Ministers

The Rt. Hon. Theresa May MP – Secretary of State for the Home Department

Other officials

Officials

SECURITY SERVICE (MI5)

Mr Andrew Parker – Director General

GOVERNMENT COMMUNICATIONS HEADQUARTERS (GCHQ)

Mr Robert Hannigan CMG – Director

SECRET INTELLIGENCE SERVICE (SIS)

Mr Alex Younger CMG – Chief

ISBN 978-1-4741-2771-4