Intelligence and Security Committee of Parliament

Privacy and Security: A modern and transparent legal framework

Intelligence and Security Committee of Parliament

Privacy and Security: A modern and transparent legal framework

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

Ordered by the House of Commons to be printed on 12 March 2015

HC 1075

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

Any enquiries regarding this publication should be sent to us at Committee@isc.x.gsi.gov.uk

Print ISBN 9781474116237
Web ISBN 9781474116244

ID 10031502 03/15 47945 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'). 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.*

CONTENTS

KEY FINDINGS

i. The internet has transformed the way we communicate and conduct our day-to-day lives. However, this has led to a tension between the individual right to privacy and the collective right to security, which has been the focus of considerable debate over the past 18 months.

ii. The leak by Edward Snowden of stolen intelligence material in June 2013 led to allegations regarding the UK Agencies' use of intrusive capabilities – in particular those relating to GCHQ's interception of internet communications. This Committee investigated the most serious of those allegations – that GCHQ were circumventing UK law – in July 2013. We concluded that that allegation was unfounded. However, we considered that a more in-depth Inquiry into the full range of the Agencies' intrusive capabilities was required – not just in terms of how they are used and the scale of that use, but also the degree to which they intrude on privacy and the extent to which existing legislation adequately defines and constrains these capabilities.

iii. All those who contributed to this Inquiry agreed that the intelligence and security Agencies have a crucial role protecting UK citizens from threats to their safety. The UK intelligence and security Agencies (MI5, SIS and GCHQ) exist to protect the country from threats and to obtain intelligence in the interests of the UK's national security or economic well-being and for the detection and prevention of serious crime. The importance of this work is reflected in the fact that Parliament has provided the Agencies with a range of intrusive powers which they use to generate leads, to discover threats, to identify those who are plotting in secret against the UK and to track those individuals.

iv. However, in a democratic society those powers cannot be unconstrained: limits and safeguards are essential. First and foremost, the Agencies are public bodies and therefore everything they do must be in accordance with the Human Rights Act 1998 (which incorporates the European Convention on Human Rights into UK law). While the Agencies work to protect our national security, they must do so while upholding our basic human rights. Some rights are not absolute: the right to privacy, for example, is a qualified right – as all the witnesses to our Inquiry accepted – which means that there may be circumstances in which it is appropriate to interfere with that right. In the UK, the legal test is that action can be taken which intrudes into privacy only where it is for a lawful purpose and it can be justified that it is necessary and proportionate to do so. The question that we have considered in relation to each of the Agencies' capabilities is whether the intrusion it entails is justified and whether the safeguards are sufficient.

v. Our Inquiry has involved a detailed investigation into the intrusive capabilities that are used by the UK intelligence and security Agencies. This Report contains an unprecedented amount of information about those capabilities, including how they are used, the legal framework that regulates their use, the authorisation process, and the oversight and scrutiny arrangements that apply. For ease of reference, we have included an overview of the Report in the next chapter and below we summarise our key findings:

- **We are satisfied that the UK's intelligence and security Agencies do not seek to circumvent the law – including the requirements of the Human Rights Act 1998, which governs everything that the Agencies do.**
- **However, that legal framework has developed piecemeal, and is unnecessarily complicated. We have serious concerns about the resulting lack of transparency, which is not in the public interest.**
- **Our key recommendation therefore is that the current legal framework be replaced by a new Act of Parliament governing the intelligence and security Agencies. This 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.**
- **Our Report also contains substantial recommendations about each of the Agencies' intrusive capabilities, which we consider are essential to improve transparency, strengthen privacy protections and increase oversight.**
- **We have scrutinised GCHQ's bulk interception capability in particular detail, since it is this that has been the focus of recent controversy:**
  - **Our Inquiry has shown that the Agencies do not have the legal authority, the resources, the technical capability, or the desire to intercept every communication of British citizens, or of the internet as a whole: GCHQ are not reading the emails of everyone in the UK.**
  - **GCHQ's bulk interception systems operate on a very small percentage of the bearers[2] that make up the internet. We are satisfied that they apply levels of filtering and selection such that only a certain amount of the material on those bearers is collected. Further targeted searches ensure that only those items believed to be of the highest intelligence value are ever presented for analysts to examine: therefore only a tiny fraction of those collected are ever seen by human eyes.**
  - **The current legal framework of external and internal communications has led to much confusion. However, we have established that bulk interception cannot be used to target the communications of an individual in the UK without a specific authorisation naming that individual, signed by a Secretary of State.**
- **While these findings are reassuring, they nevertheless highlight the importance of a new, transparent legal framework. There is a legitimate public expectation of openness and transparency in today's society, and the intelligence and security Agencies are not exempt from that.**

[2] *Internet communications are primarily carried over international fibre optic cables. Each cable may carry several 'bearers' which can carry up to 10 gigabits of data per second.*

OVERVIEW

Interception of communications

vi. While we have considered the entire range of intrusive capabilities available to the Agencies, public controversy has centred on GCHQ's interception of internet communications which some have alleged means that GCHQ are 'hoovering up' the communications of everyone in the UK. Such 'blanket surveillance' would not only be unlawful, but also unacceptable. We have therefore scrutinised GCHQ's capability to intercept internet communications in detail, including how GCHQ collect communications and the circumstances in which they may then examine those communications (paragraphs 49–128).

vii. ***Why do the Agencies intercept communications?*** The Agencies conduct two types of interception, depending on the information they have and what they are trying to achieve:

a) *As an investigative tool*. Where there is specific knowledge about a threat (e.g. a specific email address has been linked to terrorist activity), the Agencies may intercept that individual's communications, provided they can demonstrate to a Secretary of State that it is necessary and proportionate to do so. This is known as 'targeted interception' and must be authorised by a warrant signed by a Secretary of State under Section 8(1) of the Regulation of Investigatory Powers Act 2000 (RIPA). Contributors to this Inquiry broadly accepted the principle of targeted interception. (Specific aspects of 'targeted interception' – and detailed recommendations for improvements in procedures – are covered in paragraphs 28–48.)

b) *As a 'discovery', or intelligence-gathering, tool.* The Agencies can use targeted interception only after they have discovered that a threat exists. They require separate capabilities to uncover those threats in the first place, so that they can generate leads and obtain the information they need to then target those individuals. It is this 'bulk interception' capability that has led to allegations that GCHQ are monitoring the communications of everyone in the UK.

viii. ***How much of the internet do GCHQ 'hoover up'?*** We have investigated in considerable detail the processes by which GCHQ intercept internet communications in bulk. These processes involve first the collection of communications (which is authorised by a warrant signed by a Secretary of State under RIPA) and then the examination of a small number of those communications (if the material is listed in the Certificate that accompanies that warrant).

- The first of the major processing systems we have examined is targeted at a very small percentage of the 'bearers' that make up the internet. As communications flow across those particular bearers, the system compares the traffic against a list of 'simple selectors'. These are specific identifiers relating to a known target. Any communications which match are collected (paragraphs 60–64).
- Analysts must then carry out a 'triage process' to determine which of these are of the highest intelligence value and should therefore be opened and read. Only a very small proportion (***%) of the items collected under this process

(around *** items per day) are ever opened and read by an analyst. Even when GCHQ know that a communication relates to a known target, they still do not have the capacity to read all of them; they have to prioritise (paragraphs 74–75).

- Another major processing system by which GCHQ may collect communications is targeted at an even smaller number (just ***%) of the bearers that make up the internet (these are a subset of those accessed by the process just described). GCHQ apply *** 'selection rules' and, as a result, the processing system automatically discards the majority of the traffic that is carried across these bearers. The remainder – which GCHQ consider most likely to contain items of intelligence value – are collected (paragraphs 65–73).

- The processing system then runs both automated and bespoke searches on these communications in order to draw out communications of intelligence value. By performing complex searches combining a number of criteria, the odds of a 'false positive' are considerably reduced. The system does not permit GCHQ analysts to search these communications freely (i.e. they cannot conduct fishing expeditions). The complex searches draw out only those items most likely to be of highest intelligence value. These search results – around *** items per day – are then presented to analysts in list form: it is only the communications on this list that analysts are able to open and read. They cannot open any communications which have not matched the complex searches. (This can be thought of as using a magnet to draw the needle out of a haystack instead of combing through the straw yourself.) Analysts then rank the communications on the list in order of intelligence value, in order to decide which ones to examine: they open and read only a very tiny percentage of the communications collected (around *** items per day) (paragraphs 76–77).

- **GCHQ's bulk interception systems operate on a very small percentage (***%) of the bearers that make up the internet. It cannot therefore realistically be considered blanket interception.**

- **There are nevertheless still vast numbers of communications travelling across these bearers (hence it is described as bulk interception). GCHQ therefore filter this traffic still further, resulting in the collection of only a fraction of the traffic that is carried by this small number of bearers: ***.**

- **This collection is based on specific criteria and filters: GCHQ do not therefore conduct interception indiscriminately.**

- **Further, GCHQ do not open and read all the communications they collect. Collection and examination are two separate processes: only a very tiny percentage (***%) of the communications that GCHQ collect are ever opened and read by an analyst.**

- **In practice, this means that fewer than *** of *** per cent of the items that transit the internet in one day are ever selected to be read by a GCHQ analyst, and these have gone through several stages of targeting, filtering and searching so that they are believed to be the ones of the very highest intelligence value.**

ix. ***Are GCHQ reading the communications of people in the UK?*** We address this point in some detail, and provide examples, in paragraphs 105–115. However, in summary:

- **Communications between people in the UK are classed as internal communications: they can therefore only be searched for, examined and read through targeted interception, which requires the authority of an 8(1) warrant signed by a Secretary of State which names the individual being targeted.**
- **GCHQ are authorised to collect 'external' communications (where at least one end is outside the UK) under the broader authority of an 8(4) warrant signed by a Secretary of State. Of these, they are then authorised to search for and select communications to examine on the basis of a selector (such as an email address) of an individual overseas – provided that their reason for doing so is one or more of the categories described in the Certificate that accompanies the 8(4) warrant.**
- **Crucially, GCHQ can only search for and select communications to examine on the basis of a selector of an individual in the UK if – and only if – they first obtain separate additional authorisation from a Secretary of State which names that individual. It is unlawful for them to search for and examine the communications of someone in the UK without that additional targeted authorisation.**

x. ***Do they need to intercept these communications?*** While we are reassured that bulk interception is tightly drawn, it is nevertheless an intrusive capability. It is therefore essential that it is for a legal purpose, but also that it is necessary and proportionate. We have examined cases which demonstrate that this capability has been used to find communications indicating involvement in threats to national security. Bulk interception has exposed previously unknown threats or plots which threatened our security that would not otherwise have been detected (paragraphs 78–90). While we recognise privacy concerns about bulk interception as a matter of principle, we do not subscribe to the point of view voiced by some of our witnesses that it is preferable to let some terrorist attacks happen rather than to allow any form of bulk interception. It is right that the Agencies have this capability: what is important is that it is tightly controlled and subject to proper safeguards.

xi. ***Is it properly controlled and regulated?*** GCHQ must operate within the existing legal framework. Equally important is whether the existing legal framework is appropriate, particularly given changing technology and expectations about privacy. We have made a number of substantial recommendations for immediate improvements to the existing system of authorisation and oversight – we also recommend a more thorough overhaul of the legislation which we set out below. These short-term changes are broadly to address: the need for greater transparency; a more streamlined, simpler process; greater safeguards in relation to British citizens overseas, and for individuals who work in 'sensitive' professions that require privacy for their work; and increased oversight by the Interception of Communications Commissioner (we have recommended an increased role for both the Interception of Communications Commissioner and the Intelligence Services Commissioner in a number of areas covered by this Report).

Communications Data

xii. While much of the recent controversy has focused on GCHQ's interception of emails, there has also been concern over the use the Agencies make of Communications Data (CD). This encompasses the details about a communication – the 'who, when and where' – but not the content of what was said or written. CD is a critical capability for the Agencies: it is used to develop leads, focus on those who pose a threat and illuminate networks. However, concerns have been raised as to whether the distinction between data and content is still meaningful, and also whether changes in technology mean that CD is now just as intrusive as content.

xiii. In our opinion the definition of CD used in RIPA is narrowly drawn and, while the volume of CD available has made it possible to build a richer picture of an individual, this remains considerably less intrusive than content. It does not therefore require the same safeguards as content does. However, we have found this debate to be complicated by the confusion as to what information is categorised as CD and what is treated as content – particularly in relation to internet communications and web browsing histories (paragraphs 136–143).

- It is essential to be clear what constitutes CD. In particular, there is a 'grey' area of material which is not content, but neither does it appear to fit within the narrow 'who, when and where' of a communication, for example information such as web domains visited or the locational tracking information in a smartphone. This information, while not content, nevertheless has the potential to reveal a great deal about a person's private life – his or her habits, tastes and preferences – and there are therefore legitimate concerns as to how that material is protected.
- We have therefore recommended that this latter type of information should be treated as a separate category which we call 'Communications Data Plus'. This should attract greater safeguards than the narrowly drawn category of Communications Data.

Other intrusive capabilities

xiv. We have also examined a number of other intrusive capabilities that are used by the Agencies (paragraphs 151–193). These include both the explicit capabilities defined in RIPA (such as the use of surveillance and the use of agents), and those capabilities that are implicitly authorised through general provisions in the Security Service Act 1989 and the Intelligence Services Act 1994 (such as the use of IT Operations against targets overseas and the acquisition of Bulk Personal Datasets). Our Report contains a number of detailed recommendations, primarily in relation to: greater transparency, to the extent that this is possible without damaging national security; and specific statutory oversight by either the Intelligence Services Commissioner or the Interception of Communications Commissioner in those areas where oversight is currently undertaken on a non-statutory basis.

Authorisation of intrusive action

xv. The Agencies' most intrusive capabilities are authorised by a warrant or other authorisation signed by a Secretary of State, with officials authorising those capabilities considered to be less intrusive. The primary question we have considered in this area is whether Ministers or judges should sign warrants for intrusive activity. We recognise the concerns put to us by some witnesses about public trust. However, the deciding factor for us is that while both Ministers and judges can assess legal compliance, Ministers can then apply an additional test in terms of the diplomatic and political context and the wider public interest. This additional test would be lost if responsibility were transferred to judges and might result in more warrant applications being authorised. Furthermore, judges are not held accountable, or asked to justify their decisions to Parliament and the public, as Minsters are. It is therefore right that responsibility for authorising warrants for intrusive activity remains with Ministers (paragraphs 194–203).

The legislative framework

xvi. There is no one piece of legislation that governs what the intelligence and security Agencies can and cannot do: broadly, the Security Service Act 1989 and the Intelligence Services Act 1994 provide the legal basis for the Agencies' activities, but that is subject to the overarching requirements of the Human Rights Act 1998, and further constraints on certain of those activities as set out in a number of other pieces of legislation (for example, the Regulation of Investigatory Powers Act 2000). This is not just opaque, it is unnecessarily complicated. Further, it is inappropriate that many key capabilities – for example, the exchange of intelligence with international partners – are implicitly authorised rather than formally defined in statute (paragraphs 220–275).

xvii. The Committee has serious concerns about the adequacy of the current legislative framework governing and constraining the Agencies' activities. We have seen no evidence that the Agencies are seeking to circumvent the law: in fact, the care and attention given to complying with the law within the Agencies is highly commendable. But the lack of clarity in the existing laws, and the lack of transparent policies beneath them, has not only fuelled suspicion and allegations but has also meant that the Agencies could be open to challenge for failing to meet their human rights obligations due to a lack of 'foreseeability'. The adequacy of the legal framework and the greater need for transparency have been at the forefront of this Inquiry throughout.

xviii. While the Committee has concluded that the legal framework governing the Agencies' use of intrusive powers requires greater transparency, this is a political view rather than a legal judgment. The narrower question as to whether the legislation and Agencies' policies adequately meet the legal requirement for 'foreseeability' under the European Convention on Human Rights is, rightly, a matter for the Investigatory Powers Tribunal (IPT) and the European Court of Human Rights. In this respect, we note the recent IPT judgments on this issue on 5 December 2014 and 6 February 2015. Nevertheless, whatever decision the courts may reach in relation to compliance with the legal requirements of the Convention, we consider that additional improvements can and should be made as a matter of good practice.

- **While we have made specific recommendations in relation to specific capabilities throughout this Report, these are only short-term solutions: such reforms and improvements around the edges of the existing legislation are not sufficient in the long term. Rather than reforming RIPA, as some have suggested, we consider that the entire legal framework governing the intelligence and security Agencies needs replacing.**
- **The purposes, functions, capabilities and obligations of the Agencies should be clearly set out in a new single Act of Parliament. This should be distinct from legislation covering law enforcement and other bodies currently covered by RIPA: the purpose, scale and use of intrusive activities conducted by the intelligence Agencies are not the same as those conducted by the police or local authorities.**
- **We have set out the key principles which must underpin this new legal framework in detail. These are based on explicit avowed capabilities, together with the privacy constraints, transparency requirements, targeting criteria, sharing arrangements and other safeguards that apply to the use of those capabilities.**

xix. These changes are overdue. Not only is there a legal requirement of 'foreseeability' to ensure compliance with human rights law, there is also a legitimate public expectation of openness and transparency in today's society and, while the Agencies require secrecy in order to conduct much of their work, the Government must make every effort to ensure that as much information as possible is placed in the public domain. This is essential to improve public understanding and retain confidence in the work of the intelligence and security Agencies.

---

1. INTRODUCTION

1. The way we all communicate has changed dramatically in the last 25 years. In particular, the internet as a means of communication has had a significant impact on how we conduct our day-to-day lives: someone can send an email while sitting on their train on the way to work, message friends on WhatsApp throughout the day and have a video chat in the evening with relatives who live hundreds of miles away.

2. The extent to which our communications on the internet can be (and should be) accessed by others, particularly the intelligence Agencies, came into sharp focus in June 2013 when a contractor working for the National Security Agency (NSA) in the United States, Edward Snowden, stole a cache of classified material which he then shared with media outlets around the world. This led to allegations that government agencies were engaged in blanket surveillance of the internet.

3. This brought the debate on internet freedom into the limelight – to what extent should the internet be a private space for individuals to communicate? Some condemned the intelligence Agencies for what they believed to be the indiscriminate monitoring of internet services and networks. The internet, they believe, is a place where people should be free to communicate and discuss what they want, without fear that they are being 'snooped' on by the Government.

4. As a result of the Snowden allegations, technology companies have improved privacy protections and strengthened the encryption offered to their customers. The extent to which a Communications Service Provider (CSP) can assure their users that their communications cannot be read by the intelligence Agencies has become a part of their marketing strategy.[3] For example, Apple's CEO Tim Cook has issued the following statement:

> *I want to be absolutely clear that we have never worked with any government agency from any country to create a backdoor in any of our products or services. We have also never allowed access to our servers. And we never will.*[4]

However, while CSPs may be primarily concerned about commercial advantage, the growing use of encryption also raises moral and ethical issues. The effect of increased privacy controls has been to place some of the communications of their users beyond the reach of law enforcement and intelligence officers and even, in some cases, beyond the reach of the law courts: should CSPs be providing an opportunity for terrorists and others who wish to do us harm to communicate without inhibition?[5]

---

[3] *In addition to the action of technology companies, some individuals have also deliberately moved their communications to the 'Dark Web'. This is not indexed by ordinary search engines and can only be accessed anonymously through software such as 'The Onion Router' (TOR). Individuals have developed methods of accessing websites and sharing files which mask all details of what has been accessed, what messages have been sent, or which files exchanged. Some estimates claim that the 'dark' internet may be several orders of magnitude larger than the 'public' internet. While this 'Dark Web' has many positive applications, such as the use by pro-democracy activists to publicise human rights abuses and foment dissent in the world's most repressive countries, it also hosts a huge array of illegal and unethical services, such as trading guns, drugs, stolen goods and child pornography.*

[4] *http://www.apple.com/privacy/*

[5] *For example, in September 2014 both Apple and Google moved towards encrypting users' data on mobile telephones by default, using their operating systems (iOS and Android) in a way that even the companies themselves cannot decrypt. This essentially places the data on those telephones beyond the reach of any law enforcement agencies, even where they have obtained a lawful court order for access. 'Going Dark: Are Technology, Privacy and Public Safety on a Collision Course?' – Speech given by FBI Director James Comey at the Brookings Institution, 16 October 2014.*

5. In response to the actions of many CSPs, the police and intelligence agencies have begun to speak out. They have voiced concerns that their ability to monitor the internet communications of those who represent a threat to national security or public safety has been significantly reduced. The Director of the Federal Bureau of Investigation in the US, James Comey, has spoken out about the dangers of the internet 'going dark':

> *Encryption just isn't a technical feature, it's part of a marketing strategy, but it will have very serious consequences for law enforcement and national security agencies at all levels… There should be no law-free zones in this country…*[6]

6. The new Director of GCHQ drew attention, in November 2014, to the way in which the Islamic State of Iraq and the Levant (ISIL) is exploiting the power of the internet to *"create a jihadi threat with near-global reach"*. He said:

> *There is no doubt that young foreign fighters have learnt and benefited from the leaks of the past two years… However much* [technology companies] *may dislike it, they have become the command-and-control networks of choice for terrorists and criminals.*[7]

7. It is worth noting that this debate does not seem to arise in the context of the Agencies intercepting letters, or listening to people's home or office landline calls. So what is it about the internet that makes it different? For many, the free and open nature of the internet represents liberty and democracy, and they consider that these values should not be compromised for the sake of detecting a minority who wish to use it for harmful purposes.

8. However, others consider that liberty is most real where security also exists: if the internet is an ungoverned space it can also be a dangerous space, threatening the liberty of all. This was illustrated in this Committee's Report into the intelligence relating to the murder of Fusilier Lee Rigby, in which we outlined how Michael Adebowale had expressed his desire to carry out his murderous terrorist attack in an online exchange with an extremist overseas. The Agencies did not have access to this exchange before the attack: had they had access to it at the time, there is a significant possibility that MI5 would have been able to prevent the attack.

This Inquiry

9. These issues demonstrate the tension between the individual's right to privacy and our collective right to security and set the context in which this Inquiry has been conducted. Following the NSA leaks, there were serious allegations regarding the Agencies' use of their intrusive capabilities, particularly those relating to GCHQ's interception of internet communications. This Committee undertook an urgent investigation to establish if the most serious allegation – that GCHQ were circumventing the law by obtaining material from the NSA – was true. In July 2013, the Committee reported:

---

[6] *'Going Dark: Are Technology, Privacy and Public Safety on a Collision Course?' – Speech given by FBI Director James Comey at the Brookings Institution, 16 October 2014.*

[7] *Director GCHQ, Financial Times, 3 November 2014.*

It has been alleged that GCHQ circumvented UK law by using the NSA's PRISM programme to access the content of private communications. From the evidence we have seen, we have concluded that this is unfounded.[8]

10. While that investigation was narrowly focused on access to the PRISM programme underneath the existing UK law, it nevertheless highlighted wider issues: some elements of the legislative framework governing the Agencies' work are overly complex, difficult to interpret in relation to certain internet technologies, and lack transparency. We considered that there needed to be a fundamental review of the legislative framework governing the powers available to the three intelligence Agencies.

11. This Inquiry has therefore considered: the range of intrusive capabilities currently available to the Agencies; how those capabilities are used in their investigations; the scale of their use; the extent to which these capabilities intrude on privacy; and the legal authorities and safeguards that constrain and regulate their use. (While we have not focused solely on internet communications in this Report, we have spent a significant amount of time examining this issue, given the controversy surrounding GCHQ's bulk interception capabilities.) Throughout this Report we have also considered the need for greater transparency about the range of Agency capabilities and how they are used and authorised. We have questioned whether the Government's standard approach – not to comment on operational intelligence matters or capabilities – is still tenable or whether it is now time for change.

12. In carrying out this Inquiry, we are satisfied that the Committee has been informed about the full range of Agency capabilities, how they are used and how they are authorised. We have sought to include as much of this information as possible in this Report with the intention that it will improve transparency and aid public understanding of the work of the Agencies. Nevertheless, certain detail cannot be published since to do so would severely damage the Agencies' ability to protect the UK. As with our Report on the intelligence relating to the murder of Fusilier Lee Rigby, the Committee has considered every request to redact material very carefully, taking into account the public interest in revealing the information and the public interest in protecting the country. For example, while the Committee has been provided with the exact figures relating to the number of authorisations and warrants held by the Agencies, we have agreed that publishing that level of detail would be damaging to national security.

13. In response to a call for evidence, the Committee received 56 substantive submissions covering a whole range of opinions. Contributors included the Government, Parliamentarians, NGOs, privacy advocates, the media and members of the public. The Committee also received classified written evidence from the Agencies on their operational capabilities, and questioned them in detail in evidence sessions.

14. In October 2014, the Committee held a number of public evidence sessions, taking evidence from both sides of the debate. The Committee also took evidence in public from the Deputy Prime Minister in his capacity as Leader of the Liberal Democrats, the Shadow Home Secretary, and – for the first time in public – from the Home Secretary and the Foreign Secretary; and in closed session from the Interception of Communications Commissioner, the Intelligence Services Commissioner and the Home and Foreign

[8] *'Statement on GCHQ's Alleged Interception of Communications under the US PRISM Programme', Intelligence and Security Committee of Parliament, 17 July 2013.*

Secretaries.[9] We also discussed these issues in detail with the Prime Minister in December 2014.

15. Those we heard evidence from expressed a wide range of views. Nevertheless, all contributors to this Inquiry agreed that the intelligence and security Agencies have a crucial role in protecting UK citizens from threats to their safety. What is important is how they protect us, what capabilities they use, the legal framework that governs that use and how that ensures the protection of human rights.

[9] *Responses to the call for evidence and transcripts of the (public) oral evidence sessions are published on the ISC website: http://isc.independent.gov.uk/*

2. THE AGENCIES' USE OF INTRUSIVE CAPABILITIES

16. 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 UK and to obtain intelligence in the UK and overseas to that end. Their functions are set out in the Security Service Act 1989 (SSA) and the Intelligence Services Act 1994 (ISA).

17. ISA and the SSA give the Agencies the legal power to obtain and disclose information in pursuit of their statutory purposes (in the case of SIS and GCHQ) and statutory functions (in the case of MI5):

- the protection of the UK's national security;
- safeguarding the UK's economic well-being; and
- in support of the prevention and detection of serious crime.

They have access to a range of sources and techniques which they use to generate leads, to discover threats, and then to identify and investigate those who are plotting in secret against the UK.[10] This includes information that they obtain from other organisations (such as the police, other UK agencies and overseas partners), as well as intelligence gathered through the use of their own capabilities. The Director General of MI5 has described piecing together these various strands of intelligence:

> *The way intelligence collection works might be thought of as a sort of tapestry picture. Because we are weaving together different types of intelligence to try and make a picture of what is going on, and understand it and then decide what we have to do about it.*[11]

18. The Agencies' capabilities fall into two categories:

i) those which can be used only in a targeted way against specific individuals who are suspected of being a threat to the UK (such as conducting surveillance or intercepting an individual's telephone line or email address); and

ii) those which involve the Agencies casting their nets wider and analysing large volumes of information, which enable the Agencies also to find linkages, patterns, associations or behaviours which might demonstrate a serious threat requiring investigation. (These capabilities nevertheless require some degree of targeting in order to ensure that a human eye only looks at that which is most likely to be of intelligence value.)

19. Over the course of this Inquiry, the Committee required the Agencies to provide comprehensive information about the capabilities that are available to them. We took evidence on the following:[12]

---

[10] *SIS and GCHQ also have intelligence requirements to protect UK forces deployed around the world, and to obtain secret intelligence on critical global security and economic issues.*

[11] *Oral Evidence – MI5, 8 May 2014.*

[12] *The police also use a number of these capabilities, but we have not examined their processes. We note that the Home Affairs Select Committee published a report on RIPA, in December 2014, which addressed how the police use the capabilities set out in RIPA.*

- Targeted Interception of Communications;
- Bulk Interception of Communications;
- Accessing Communications Data;
- Bulk Personal Datasets;
- 'Intrusive Surveillance' (conducted inside a person's home, hotel room, car or other private place);
- 'Directed Surveillance' (in a public place);
- Interfering with Property (personal possessions or specific premises);
- IT Operations[13] – gaining (what would otherwise be unauthorised) access to, or interfering with, computing devices;
- Interfering with Wireless Telegraphy (e.g. radio signals); and
- Covert Human Intelligence Sources, otherwise known as 'agents'.

20. Each of the Agencies' capabilities has the potential to intrude into the privacy of their Subjects of Interest (SoIs)[14] to a greater or lesser extent – and generally the more intrusive the capability, the higher the level of authorisation required. However, the Agencies are of course subject to legal constraints and do not have authority to take whatever action they deem necessary in order to carry out their functions. Their actions – and their use of intrusive capabilities – are circumscribed by the requirements of the Human Rights Act 1998 (HRA).

The Human Rights Act 1998

21. The HRA imposes a duty on all UK public authorities (including the Agencies) to act in a way that complies with the European Convention on Human Rights (ECHR): Section 6 of the HRA states that *"it is unlawful for a public authority to act in a way which is incompatible with a Convention right"*. Therefore, while the Agencies work to protect our fundamental right to life (as enshrined in Article 2 of the ECHR), they must pursue that work in a manner that is consistent with other Convention rights, such as the right to liberty and security of person (Article 5), the right to freedom of expression (Article 10) and – crucially in terms of this Inquiry – the right to privacy (Article 8).

---

[13] *The Agencies use the term 'Equipment Interference' rather than 'IT Operations'. The draft 'Equipment Interference Code of Practice' (published by the Home Office on 6 February 2015) explains that this may include interference with computers, servers, routers, laptops, mobile phones and other devices "in order to do any or all of the following:*
a. obtain information from the equipment in pursuit of intelligence requirements;
b. obtain information concerning the ownership, nature and use of the equipment in pursuit of intelligence requirements;
c. locate and examine, remove, modify or substitute hardware or software which is capable of yielding information of the type described in a) or b);
d. enable and facilitate surveillance activity by means of the equipment".

[14] *An SoI is an individual investigated by the Agencies because they are suspected of being a threat to national security.*

THE EUROPEAN CONVENTION ON HUMAN RIGHTS

Article 2 states:

(1) Everyone's right to life shall be protected by law. No one shall be deprived of his life intentionally save in the execution of a sentence of a court following his conviction of a crime for which the penalty is provided by law.

(2) Deprivation of life shall not be regarded as inflicted in contravention of this Article when it results from the use of force which is no more than absolutely necessary:

a) in defence of any person from unlawful violence;

b) in order to effect a lawful arrest or to prevent the escape of a person lawfully detained;

c) in action lawfully taken for the purpose of quelling a riot or insurrection.

Article 8 states:

(1) Everyone has the right to respect for his private and family life, his home and his correspondence.

(2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

22. The right to privacy is a qualified right – i.e. it may be interfered with in order to safeguard other human rights, whether of the individual or of society as a whole. All those who contributed to our Inquiry acknowledged this. However, the challenge for any democracy is to determine the precise interaction between these rights.

The HRA 'triple test'

23. There are clearly circumstances in which an individual's right to privacy may be incompatible with our collective right to security, and one right must take precedence over the other. This interaction is managed through what is called the HRA 'triple test', which must be passed before action can be taken which compromises an individual's right to privacy. Witnesses to this Inquiry explained that the HRA 'triple test' is based on the qualifications to the ECHR right to privacy (i.e. that any intrusion must be justified *"in accordance with the law"* and *"necessary in a democratic society"*), combined with European jurisprudence. The Ministry of Justice guide to the Human Rights Act explains that a public authority can interfere with Article 8 rights if it can be shown that:

> *... the interference had a clear legal basis; the aim of the interference was either national security, public safety, protection of the economy, prevention of crime, the protection of health or morals or the protection of the rights and freedoms of others; it was necessary (and not just reasonable) to interfere with your rights for one of the permitted reasons; and that the interference was proportionate, going only as far as was required to meet the aim.*[15]

[15] *'A Guide to the Human Rights Act 1998', Third Edition, Ministry of Justice, October 2006.*

24. The 'triple test' has been incorporated into various UK legislation, although the precise articulation varies. For example, Section 7 of the Intelligence Services Act 1994 talks of Ministerial authorisation where action is for the *'proper discharge of a function'*, *'necessary'* and *'reasonable'*; while the Regulation of Investigatory Powers Act 2000 uses slightly different wording, requiring a Secretary of State to assert that the conduct sought under a warrant is:

- *'for a lawful purpose'* – for the Agencies this means it has to be in the interests of national security, to safeguard our economic well-being, or for the prevention and detection of serious crime;[16]
- *'necessary'* – i.e. the intrusion must be necessary for one of the purposes listed above; and
- *'proportionate'* – i.e. the action must be no more intrusive than is justified for the purpose of the investigation, and must not unnecessarily intrude on the privacy of innocent people.

In determining whether it is necessary and proportionate, it must be considered whether the information could reasonably be obtained by other means.

25. Those who gave evidence to this Inquiry agreed in principle that this HRA 'triple test' provides an appropriate basis for determining the circumstances in which it is appropriate to interfere with a Convention right such as privacy. However, many expressed serious concerns about how the test was applied in practice (whether this was by the Agencies themselves or by the Government Ministers who approve the use of the most intrusive capabilities).

26. During the course of this Inquiry we have therefore considered how the 'triple test' is applied in relation to each of the capabilities used by the Agencies, how Ministers assure themselves that the 'tests' have been applied properly, and how those decisions are reviewed such that Ministers (and the Agencies) are held accountable for their decisions.

27. We have also examined where there is scope for greater transparency about the Agencies' capabilities. We recognise that much of the Agencies' work must remain secret if they are to protect us effectively. However, given that their work may infringe ECHR rights such as privacy, we consider it essential that the public are given as much information as possible about how they carry out their work, and the safeguards that are in place to protect the public from unnecessary or inappropriate intrusion.

[16] *The Data Retention and Investigatory Powers Act 2014 clarified that interception warrants can only be issued, and Communications Data can only be obtained, to safeguard economic well-being when it is also to protect national security.*

3. TARGETED INTERCEPTION OF COMMUNICATIONS

- Interception is the monitoring of a communication in the course of its transmission so as to make some or all of its contents available to someone other than the sender or intended recipient.
- The interception of an individual's communications provides the content of those communications (what was said or written) as well as communications data about the communication (the 'who, when and where').
- This chapter is about content: Communications Data is considered in Chapter 6.

28. Where the Agencies consider that a known individual may pose a threat to the UK, or be of legitimate intelligence interest to them, they may seek authority to intercept that suspect's communications – provided they can demonstrate that it is both necessary and proportionate to do so.[17] Twenty-five years ago this might have included recording their conversations on their telephone landline or copying any letters that they sent by post. However, given technological advances, this may now include collecting any internet traffic that goes through their broadband connection or smartphone, or collecting emails or other communications from the internet services that they use (e.g. webmail or messaging services such as Gmail or WhatsApp).[18]

How do the Agencies carry out Targeted Interception of Communications in the UK?

29. The standard route by which the Agencies gain access to the communications of SoIs is by the relevant government department (e.g. the Home Office) serving an interception warrant on the Communications Service Provider (CSP) concerned. The CSP is then required to intercept the specific communications made by that SoI using a specific electronic identifier (e.g. a mobile telephone number or email address), and to provide them as a near-live stream directly into National Technical Assistance Centre (NTAC) systems or, in some cases, directly to the Agencies.

THE NATIONAL TECHNICAL ASSISTANCE CENTRE

NTAC was established in 2001. It has four main roles: interception of communications; enhancement of intercepted data; decryption of seized media; and advice to the Government and industry. NTAC forms part of GCHQ but serves the UK intelligence and security Agencies and police forces, as well as HM Revenue and Customs and the National Crime Agency. NTAC is located in Thames House and staffed mainly by GCHQ personnel, with secondees from other Agencies.

[17] *Some of those who provided evidence to this Inquiry referred to targeted interception on the grounds of 'reasonable suspicion'. We note, however, that such terminology is not used in current interception legislation, which contains specific tests as outlined in paragraph 24.*

[18] *We cover in more detail the different kinds of internet services people may use to communicate in the next chapter on bulk interception.*

30. The Agencies and CSPs use NTAC because it is easier for the CSPs to work with one single body (rather than a number of different organisations) and because NTAC is able to process these communications to a consistent standard (before passing them on to the Agencies).[19]

31. As a snapshot of this capability, on 8 July 2014 approximately half of all devices being monitored by NTAC were on behalf of the Agencies – *** devices for MI5 and *** devices for GCHQ.[20] (The majority of other devices being monitored that day were on behalf of the police and other law enforcement agencies.) The Agencies have said these figures are typical for any given day.

INTERCEPTION WHEN CSPs ARE BASED OVERSEAS

UK CSPs comply with interception warrants under RIPA, and NTAC maintains a relationship with all UK CSPs to facilitate this. However, individuals are increasingly communicating using services provided by CSPs based overseas.[21] In our previous Report on the intelligence relating to the murder of Fusilier Lee Rigby, this Committee discussed the difficulties faced by the Agencies in carrying out targeted interception when it involves an overseas CSP; this is because overseas CSPs generally do not comply with UK interception warrants (although recent legislation – the Data Retention and Investigatory Powers Act, passed in 2014 – compels CSPs to comply, the Government has not, as yet, sought to enforce compliance). This is having a significant impact on the Agencies' ability to use this capability. As our introduction to this Report has outlined, protection of their users' privacy is increasingly a market differentiator for technology companies and therefore (generally) they are not willing to cooperate with UK intelligence Agencies.[22]

Authorisation of Targeted Interception of Communications

32. The Agencies must seek authorisation from a Secretary of State to conduct targeted interception. This takes the form of a warrant as described in Section 8(1) of the Regulation of Investigatory Powers Act 2000 (RIPA).[23] The warrant removes liability for criminal prosecution for interception, which would otherwise be an offence under Section 1 of RIPA. The Home Secretary is responsible for signing 8(1) warrants for MI5 (or the Secretary of State for Northern Ireland in respect of warrants relating to Northern Ireland terrorism). The Foreign Secretary is responsible for signing 8(1) warrants for GCHQ and SIS.[24] (Authorisation processes more generally are discussed in Chapter 9.)

---

[19] *In some limited circumstances, MI5 may seek to engage directly with a CSP regarding an interception request (rather than go through NTAC) if there is a non-routine operational reason which necessitates direct contact.*

[20] *SIS were unable to provide equivalent figures.*

[21] *That is, companies registered and with headquarters based outside the UK.*

[22] *As we made clear in our Report on the intelligence relating to the murder of Fusilier Lee Rigby, overseas CSPs may cooperate with UK intelligence Agencies in very limited circumstances where they assist under ECPA (Electronic Communications Privacy Act) emergency criteria.*

[23] *Targeted interception of communications is lawful if the Secretary of State issues an interception warrant under Section 5(1) of RIPA. The requirements of the warrant are set out in Section 8(1) and therefore this type of warrant is commonly referred to as an 8(1) warrant.*

[24] *Warrants may be signed by any Secretary of State but they would usually be signed by the Home Secretary, the Secretary of State for Northern Ireland or the Foreign Secretary.*

33. When an Agency establishes that they need to intercept an individual's communications, they prepare a draft application for an interception warrant. This draft application goes through several levels of scrutiny within both the relevant Agency and government department, which means that before an application reaches the Secretary of State it will have been seen and possibly redrafted several times, including by lawyers and senior officials.[25]

34. The Interception of Communications Commissioner has set out a detailed explanation of the warrantry process in his 2013 Annual Report. The Commissioner's explanation is clear and provides useful detail: the Committee has reproduced the relevant sections of his Report at Annex B.

What does an 8(1) warrant look like?

35. An 8(1) warrant authorises the interception of the communications of a named individual or a single set of premises.[26] These warrants are primarily used for interception in the UK. (They may also be used for interception overseas if this is practical.[27]) Such interception must comply with human rights principles – i.e. that it is for a lawful purpose, necessary and proportionate. MI5 have explained that when they apply to the Home Secretary or the Secretary of State for Northern Ireland for an 8(1) warrant, that application specifically addresses whether it is:

i) For a lawful purpose

- How the submission relates to MI5's statutory functions, including the threat that is being investigated, the SoI's relevance to the investigation and the priority of the submission.

ii) Necessary

- How the communications to be intercepted were identified, and the intelligence that the Agencies expect to obtain from the interception.
- How the test of necessity will be met, including why the intelligence sought cannot be obtained by less intrusive means.

iii) Proportionate

- How the test of proportionality will be met, including the likely extent of any interference with the privacy of the SoI, any collateral intrusion into the privacy of others and what measures will be taken to mitigate collateral intrusion where possible.
- How information will be shared.
- Whether the intercepted material is likely to contain any confidential journalistic material, confidential personal information or information protected by legal professional privilege, and if so how such material will be handled.

---

[25] *Additional safeguards are set out in Section 15 of RIPA and the 'Interception of Communications Code of Practice', 2007. (The Government published an updated 'Interception of Communications Code of Practice' for consultation on 6 February 2014.)*

[26] *Thematic warrants are discussed in paragraphs 42–45.*

[27] *For example, through a CSP Head Office in the UK.*

36. The Committee has seen a number of applications for an 8(1) warrant and is reassured at the level of detail contained within them. It is clear that MI5 consider and assess the necessity and proportionality of the interception in detail. The Committee considered that the public would be reassured by the amount of information contained in a warrant application. However, the current legislation contains a broad prohibition regarding the disclosure of information about specific warrants and we are therefore unable to publish examples. We have instead published the template for an 8(1) warrant application, which sets out the information which must be included and the privacy and security considerations which must be addressed. (This is included at Annex C.)

37. While among the intelligence Agencies MI5 make most use of 8(1) warrants, GCHQ and SIS also seek 8(1) warrants. These applications take a slightly different form, as the detail is contained in a submission to the Foreign Secretary. They contain a good level of detail in relation to the threat being investigated, and cover all aspects required by law. However, the Committee notes that such submissions are less structured and therefore may not directly address all the detailed considerations covered in an MI5 8(1) warrant application.

38. In addition to naming or describing the subject of the interception, a Section 8(1) warrant must also list the 'selectors' (i.e. email address, postal address, telephone number etc.) which are to be used to identify the communications that are to be intercepted. These selectors must be listed in a schedule to the warrant (they may be added to or deleted through a formal amendment process).[28]

39. The warrant is forward-looking – i.e. interception can only begin once the warrant has been signed by the Secretary of State. An 8(1) warrant does not, therefore, authorise the Agencies to collect any communications sent or received prior to the date that the warrant is signed.[29]

40. Warrants are valid for six months (three months where required for the prevention and detection of serious crime), automatically lapsing at the end of six months. However, they should be cancelled sooner if they are no longer necessary and proportionate, or they may be renewed by the Secretary of State for a further six-month period if they remain necessary and proportionate. In relation to the warrants obtained by MI5 during 2013, just over half were cancelled within the initial six-month period; the remainder were renewed on at least one occasion.[30]

41. The total number of new Section 8(1) warrants issued in 2013 was 2,757. (The number of extant Section 8(1) warrants as at 31 December 2013 was 1,649.) These include all nine bodies authorised to conduct interception under RIPA. We have been given the number of 8(1) warrants for MI5, SIS and GCHQ (***, *** and *** respectively).[31] However, we cannot publish these figures since they would provide an indication of the Agencies' investigatory capacity.

---

[28] *The list of selectors may be modified by a Secretary of State, or by a senior official acting on their behalf (where this is specifically authorised in the warrant).*

[29] *In certain circumstances, ***.*

[30] *Written Evidence – MI5, 27 November 2014.*

[31] *The figure given by SIS relates to the year to July 2014 rather than the calendar year 2013.*

Thematic warrants

42. While the very significant majority of 8(1) warrants relate to one individual, in some limited circumstances an 8(1) warrant may be thematic. The term 'thematic warrant' is not one defined in statute. However, the Home Secretary clarified that Section 81(1) of RIPA defines a person as *"any organisation or any association or combination of persons"*, thereby providing a statutory basis for thematic warrants. The Home Secretary explained that *"the group of individuals must be sufficiently defined to ensure that I, or another Secretary of State, is reasonably able to foresee the extent of the interference and decide that it is necessary and proportionate"*.[32]

43. MI5 have explained that they will apply for a thematic warrant *"where we need to use the same capability on multiple occasions against a defined group or network on the basis of a consistent necessity and proportionality case… rather than* [applying for] *individual warrants against each member of the group"*.[33] The circumstances in which the Agencies might use a thematic warrant include:

- a communications address/set of premises is being used by a number of SoIs belonging to an identifiable group;
- a group of individuals are linked by a specific intelligence requirement and the case for each warrant would be more or less identical;
- interference with privacy is minimal and the national security requirement is strong enough that the Secretary of State authorises all future interference, without having to consider individual applications;
- where a high profile event is taking place attended by a large group of people of potential national security interest, but their identities are not known until the last minute; or
- the operation is fast-moving and the Agencies need flexibility to add new SoIs at short notice to prevent an attack.[34]

44. The Director General of MI5 explained that a thematic 8(1) warrant may need to be used, for example, when a group of SoIs are being investigated under the same operation ***. In such circumstances, MI5 would apply for a warrant to cover all the SoIs in the operation ***:

> ***.[35]

45. The Committee heard evidence from the Interception of Communications Commissioner's Office that they have *"made some strong recommendations around the management of thematic warrants"*.[36] The main concern appears to be that in some instances thematic warrants have been too broadly applied: on occasion, this has led the Interception of Communications Commissioner to recommend that a thematic warrant is cancelled.

---

[32] *Written Evidence – Home Secretary, 10 December 2014.*

[33] *Written Evidence – MI5, 27 November 2014.*

[34] *This is in relation to not only 8(1) warrants, but also other types of authorisations such as a Property and Intrusive Surveillance Warrant. (This is covered in Chapter 8.)*

[35] *Oral Evidence – MI5, 8 May 2014.*

[36] *Oral Evidence – Interception of Communications Commissioner's Office, 30 October 2014.*

OTHER MEANS OF ACCESSING COMMUNICATIONS CONTENT

In a small number of cases, the Agencies can access the content of communications themselves (rather than via NTAC). In these circumstances, while the Agencies may be gathering the same information, they are not conducting targeted interception as outlined in RIPA. However, they do still need to obtain the appropriate lawful authority.

i) 'SIS targeted interception overseas': Since 2013, SIS have carried out several operations relating to *"***"*.[37] These capabilities are authorised under an overarching warrant for external communications,[38] with each specific operation using these capabilities then subject to another more specific authorisation from the Foreign Secretary (these warrants are covered in detail in Chapter 5).

   In addition, SIS have a capability *** which is authorised under the Intelligence Services Act 1994. ***.[39] While this specific capability has not been deployed in the last three years, ***. [40]

ii) Interception of other types of communications: In some circumstances, the Agencies can carry out interception of communications which are not carried by public or private telecommunications systems. For instance, GCHQ can intercept radio networks used by some extremist groups. This is authorised under the Wireless Telegraphy Act 2006. Such authorisation is provided by the Secretary of State; however, no time limit is applied.[41] It appears that the intercept obtained under the authority of this Act does not fall under the statutory functions of either the Intelligence Services Commissioner or the Interception of Communications Commissioner.

iii) ***. Depending on the techniques used, the activity would be authorised by either a Property Warrant (PW) or a combined Property and Intrusive Surveillance Warrant (PSW), signed by a Secretary of State.

iv) One or both party consent: Interception can take place with the consent of one or both parties. For example, a CHIS[42] may consent to their communications being intercepted for the purpose of ensuring their safety. In this instance, a Directed Surveillance Authorisation is required under RIPA (this may be authorised internally within the Agencies).

v) Eavesdropping device: If a telephone conversation takes place in a car (or other private space, for example a bedroom) in which the Agencies have already placed an eavesdropping device (under a PSW signed by a Secretary of State), no further authorisation is required to record telephone conversations which take place within that space.

---

[37] *Written Evidence – SIS, 2 December 2014.*

[38] *This is a RIPA 8(4) warrant, discussed in Chapter 5.*

[39] ***.

[40] *Written Evidence – SIS, 27 November 2014.*

[41] *GCHQ do provide annual updates to the Secretary of State indicating the intelligence benefit obtained from the authorisations, therefore providing a justification for their continuation. For example, in relation to counter-terrorism they noted that: "Intelligence derived from data obtained under this authorisation helped track *** extremists ***". (Written Evidence – GCHQ, 21 August 2014.)*

[42] *A CHIS refers to 'Covert Human Intelligence Sources' (as defined in RIPA). They are more commonly referred to as 'agents'.*

vi) Interception within a prison: Under RIPA, a prison Governor has authority to order interception of prison telephones ***.[43]

vii) Bulk interception: GCHQ have bulk interception capabilities (which MI5 and SIS can sometimes utilise). This is discussed in detail in the next two chapters.

Collateral intrusion

46. Contributors to this Inquiry broadly accepted the principle of targeted interception on the basis of 'reasonable suspicion' (e.g. where there is specific intelligence that an individual may pose a direct threat to the UK).

47. However, one specific privacy concern was raised in relation to this capability – even when targeted interception is carried out under an 8(1) warrant, this may still result in collateral intrusion (i.e. interception of the communications of an individual other than the target). For example, when intercepting an SoI's phone this will include their calls with innocent individuals.

48. A certain degree of collateral intrusion may be inevitable, and RIPA Section 5(6) specifically allows for this. However, the extent to which the Agencies recognise and respond to this concern is important. In some circumstances, the Agencies can use other capabilities to help minimise the level of collateral intrusion (for example, ***). MI5's 8(1) warrant applications must specifically assess the probable extent of interference with the privacy of individuals who are not the subject of the warrant. Therefore, the potential for collateral intrusion is something which the Home Secretary takes into account when asked to authorise an application. In addition, MI5 have told the Committee that:

> *Collateral intrusion, the unintended, unavoidable "by product" of gathering the required intelligence, must… be considered within the total interference, and should be minimised where possible.*[44]

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).

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.

---

[43] ***.

[44] *Written Evidence – MI5, 4 March 2014.*

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.

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.

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.

4. 'BULK' INTERCEPTION: CAPABILITY

- ➢ 'Bulk' interception refers to GCHQ's capability to intercept communications primarily for intelligence-gathering purposes (as opposed to targeted investigation of known threats or people).
- ➢ 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).
- ➢ GCHQ's bulk interception capability is used:
  - 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.
- ➢ Bulk interception involves three stages of filtering, targeting and selection:
  a. choosing which communications links to access;
  b. selecting which communications to collect from those links that are being accessed; and
  c. deciding which of the collected communications should be read, analysed or examined, and stored for further analysis.

49. The targeted capabilities referred to in the previous chapter are deployed against a person or single set of premises (primarily in the UK) where there is specific knowledge about a threat (e.g. a specific email address that has been linked to terrorism or other intelligence requirements). However, the Agencies can only undertake such targeted investigation once they have discovered that a threat exists.

50. This chapter addresses the Agencies' capabilities to uncover these threats – whether that might be cyber criminals, nuclear weapons proliferators, ISIL terrorists or serious criminals – so that they can generate leads and obtain the information they need to target these individuals.

51. The Government's submission to this Inquiry explained the importance of gathering information to generate leads and enable threats to national security to be investigated:

> *In order to identify, understand and counter national security threats facing the UK, our Agencies need information… They must also be able to generate and quickly assess new leads that could reveal emerging threats… This may require the Agencies to sift through 'haystack' sources – without looking at the vast majority of material that has been collected – in order to identify and combine the 'needles' which allow them to build an intelligence picture.*[45]

[45] *Written Evidence – HMG, 7 February 2014.*

52. These leads can be generated by members of the public contacting the authorities, discovered as a by-product of MI5 or police investigations into other people or networks, reported by an agent, from an overseas intelligence agency or – increasingly – from interception of communications.

53. Twenty-five years ago the volume of communications that the Agencies could intercept in order to draw out 'unknown' threats was relatively small – for example, letters, landline telephone calls, faxes and telexes. However, the majority of communications now take place over the internet. This includes emails, internet browsing, social networking, peer-to-peer sharing sites, chat rooms, webcams, online gaming platforms, mobile applications and a whole host of other media; even 'traditional' landline and mobile telephone calls may now be carried over the internet.

54. Just as the number of different forms of communication has grown, so too has the number of communications itself. So, for example, 25 years ago a person's private communications might have consisted of a handful of telephone calls per day, and sending or receiving a few letters or postcards each week. Nowadays, with the internet playing a central role in most people's lives and the prevalence of mobile smartphones, the volume of private communications we undertake each day has grown perhaps a hundred-fold. Today, our daily communications may involve voice calls, text messages, emails, social media posts, checking news or weather apps, online shopping, online banking and other web browsing, plus a large number of background services on our phones communicating all the time without our knowledge.[46]

55. The internet carries the communications of 2.4 billion internet users. In one minute those 2.4 billion transfer 1,572,877 gigabytes of data, including 204 million emails, 4.1 million Google searches, 6.9 million messages sent via Facebook, 347,222 posts to Twitter and 138,889 hours of video watched on YouTube.[47] The vast majority of internet communications are carried around the world by high-capacity fibre optic cables (with other technologies, such as satellite or microwave links, used in certain areas). Each cable may carry multiple 'bearers',[48] and there are approximately 100,000 such bearers joining up the global internet.

56. Amongst the everyday internet usage of billions of people carried over these bearers, a very small proportion will relate to threats to the national security of the UK and our allies. In order to find these communications, the Agencies take different approaches depending on the location of their targets. Within the UK, the Agencies have

---

[46] *While smartphones are seemingly in a dormant standby state, they are constantly exchanging and synchronising data with the providers of the various applications installed on the device (such as internet messaging services, social media, email apps etc.). The provider of the operating system, or manufacturer of the device, may also have installed services that run in the background – such as those that frequently communicate your location to companies such as Google, Apple, Microsoft or others. These 'standby' services and applications obtain consent for the communications they make during installation or initial set-up (although many users do not review these in any detail before agreeing to them and may not be aware of them).*

[47] *'What happens in an internet minute?', Intel Corporation, 5 December 2014.*

[48] *GCHQ explained that the internet is carried on physical cables that are laid on the sea bed or underground: "These are quite big (typically 69mm in diameter, or about as thick as your wrist) and heavy (10kg per metre). They are made up of a series of layers (polyethylene on the outside, mylar tape and stranded steel wire to provide strength, aluminium to keep out water and polycarbonate to protect the heart of the cable, which consists of a copper tube filled with petroleum jelly in which sit a small number of optical fibres). These fibres carry the data. In one transatlantic cable for example, there are eight fibres (arranged as four pairs). These are used in a way that allows them to carry 47 separate bearers, each operating at 10 [gigabits per second ('giga-' means one thousand million, and 'bit' means binary digit)]. You could think of these bearers as analogous to different television channels – there are various ways of feeding multiple bearers down a single optical fibre, with the commonest being to use light of different frequencies. Technology is evolving fast, and there are cables planned for the near future which will contain six pairs of optical fibres, each capable of handling 100 bearers operating at 100 [gigabits per second]". (Written Evidence – GCHQ, 7 January 2015.) This means that in future, if fully loaded, a single cable could carry more traffic than 20 of the current cables.*

more opportunities to discover those threats (for example, police community officers may be approached by members of the public with leads). Interception is therefore used as an investigative tool, to find communications relating to a known threat (as set out in the previous chapter). Outside the UK, however, the opportunities to discover threats are more limited and therefore interception is used primarily as an intelligence-gathering tool.[49] This 'bulk interception' is explained below, with legal considerations and privacy concerns detailed in the next chapter.

Choosing which communications links to access

57. The allegation arising from the NSA leaks is that GCHQ 'hoover up' and collect all internet communications. Some of those who gave evidence to this Inquiry said 'the Agencies are monitoring the whole stream all the time', referring to the 'apparent ubiquity of surveillance'.

58. We have explored whether this is the case. It is clear that both for legal reasons and due to resource constraints it is not: GCHQ cannot conduct indiscriminate blanket interception of all communications. It would be unlawful for them to do so, since it would not be necessary or proportionate, as required by RIPA.[50] Moreover, GCHQ do not have the capacity to do so and can only cover a fraction of internet communications:[51]

- Of the 100,000 'bearers' which make up the core infrastructure of the internet, GCHQ could theoretically access communications traffic from a small percentage (***).[52] These are chosen on the basis of the possible intelligence value of the traffic they carry.[53]
- However, the resources[54] required to process the vast quantity of data involved mean that, at any one time, GCHQ access only a fraction of the bearers that they have the ability to access – around ***. (Again, these are chosen exclusively on the basis of the possible intelligence value of the traffic they carry.)
- In practice, GCHQ therefore access only a very small percentage (around ***%) of the internet bearers at any time.
- Even then, this does not mean that GCHQ are collecting and storing all of the communications carried on these bearers – the processes by which GCHQ select which communications to collect are covered in the next section.

59. The proportion of bearers making up the internet that are accessed by GCHQ's 'bulk interception' systems is very small – and certainly far from the 'blanket' coverage of all communications that some are concerned is happening. Nevertheless, the volume of communications flowing across these bearers, and the number of people those communications relate to, is still extremely large. We therefore consider that 'bulk' remains an appropriate term to use when describing this capability.

---

[49] *We consider the rationale behind the differences in the two regimes in greater detail in Chapter 5.*

[50] *GCHQ have no legal entitlement to use bulk interception in relation to internal (i.e. UK-to-UK) communications – the legal authorisation process is covered in the next chapter.*

[51] *Statistics derived from Written Evidence – GCHQ, 10 July 2014.*

[52] *These figures were correct as at June 2014. However, the rapid growth and development of the internet means that these figures will vary over time ***. While the number of communications links that GCHQ can access can increase or decrease over time, the overall trend is upwards. 40% of the links that GCHQ can access enter or leave the UK, with 60% entirely overseas. (***.)*

[53] *To establish this, GCHQ conduct periodic surveys, lasting a few seconds or minutes at a time, on these bearers. ***. (Written Evidence – GCHQ, 13 January 2015.)*

[54] *This includes both technical and analytical capability and affordability.*

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.**

Selection of communications to be collected

60. In addition to the concern that GCHQ are conducting 'blanket' interception of internet communications, a number of submissions to our Inquiry suggested that GCHQ's bulk interception is 'indiscriminate' and that innocent people's communications are being collected. Privacy campaigners agreed that targeted surveillance was acceptable, but found bulk interception unacceptable because they understood it to be untargeted. We have examined in detail the various processes through which GCHQ conduct bulk interception: ***.

***

61. One of the major processing systems operates on all those bearers which GCHQ have chosen to access (approximately ***) out of those they can theoretically access. As the internet traffic flows along those chosen bearers (***), the system compares the traffic against a list of specific 'simple selectors' (these are specific identifiers – *** – relating to a target). GCHQ currently have approximately *** such selectors, relating to approximately *** individual targets.[55]

62. ***.

63. Any communications which match the specific 'simple selectors' are automatically collected. All other communications are automatically discarded.[56] Each day, out of the *** billions of communications that are carried by the chosen bearers, only approximately *** items are collected. (We explore later in this chapter the extent to which these collected communications might subsequently be read or examined by GCHQ analysts.)

64. In practice, while this process has been described as bulk interception because of the numbers of communications it covers, it is nevertheless targeted since the selectors used relate to individual targets: ***.[57]

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,

---

[55] *Written Evidence – GCHQ, 23 June 2014.*

[56] *GCHQ also collect all the Communications Data associated with these communications (described as 'Related Communications Data' in RIPA) before extracting that which is most likely to be of intelligence value. We return to this issue in Chapter 6.*

[57] *Almost all of the 'simple selectors' relate to ***. However, GCHQ also search for a small number of ***. ***.*

in order to collect communications from those bearers. This interception process does not therefore collect communications indiscriminately.

***

65. Another major processing system by which GCHQ may collect communications is ***, where GCHQ are looking to match much more complicated criteria with three or four elements, for example.[58] Unlike the simple selectors used in the first process, this technique requires ***.

66. This process operates across a far smaller number of bearers – GCHQ choose just *** of the bearers out of those they can theoretically access.[59] These bearers are not chosen at random: they are deliberately targeted as those most likely to carry communications of intelligence interest. (For example, GCHQ are currently targeting bearers likely to be carrying communications of ***.)

67. As a first step in the processing under this method, ***. *** the system applies a set of 'selection rules'. As of November 2014, there were *** selection rules. ***. Examples of these initial selection rules are:

- include ***;
- include ***; and
- discard communications ***.[60]

As a result of this selection stage, the processing system automatically discards the majority (***) of the traffic on the targeted bearers. The remainder is collected ***.[61] These communications are the ones that GCHQ consider most likely to contain items of intelligence value.[62, 63]

68. ***.[64]

69. GCHQ's computers then perform automated searches using complex criteria (***) to draw out communications of intelligence value. By performing searches combining a number of criteria, the odds of a 'false positive' are considerably reduced. ***.[65]

70. While analysts may create additional bespoke searches based on the complex criteria, the system does not permit them to search freely (i.e. they cannot conduct fishing expeditions). GCHQ explained: *"***"*.[66]

71. The individual communications which match these complex searches number approximately *** items per day. These are made available, in list form, to analysts for

---

[58] *GCHQ have a number of other capabilities of this type, including: ***.*
[59] *These are a subset of the same bearers that are accessed under the method already described.*
[60] *Written Evidence – GCHQ, 14 November 2014.*
[61] *Written Evidence – GCHQ, 10 July 2014.*
[62] *Written Evidence – GCHQ, 10 July 2014.*
[63] *These are the items which GCHQ have determined include communications relevant to one of GCHQ's statutory functions.*
[64] *Written Evidence – GCHQ, 14 November 2014.*
[65] *Written Evidence – GCHQ, 28 February 2014.*
[66] *Written Evidence – GCHQ, 14 November 2014.*

possible examination and storage (we consider the criteria for examination later in this chapter).[67]

72. The content of all communications *** is deleted ***. The Communications Data (CD) relating to these communications is deleted ***.[68] (We explain CD in Chapter 6.)

73. In summary, collection via this alternative method means that GCHQ *** collect a very significant number of communications each day. However, this is not indiscriminate:

- GCHQ have first chosen specific bearers to access, based on those most likely to be carrying relevant communications: they choose only a small proportion of those that GCHQ are theoretically able to access, of the 100,000 comprising the internet.
- Selection rules are applied to the traffic on these bearers. (***.)
- Communications matching the selection rules *** amount to approximately *** communications per day.
- The system then processes the items ***.
- Highly complex searches (both automated and bespoke) relevant to GCHQ intelligence requirements are run against the items *** to draw out communications most likely to be of greatest intelligence value. These searches generate a list, or index, of communications, from which analysts can then decide which communications to examine. This list comprises approximately *** items per day. Analysts cannot examine any other communications.

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.

Deciding which of the collected communications to examine or read

***

74. In terms of the first method we have analysed, the use of simple selectors ensures that items collected relate to specific individual targets. However, this still represents too many items for analysts to examine, so they must then carry out a 'triage' process to determine which will be of most use.

---

[67] *Written Evidence – GCHQ, 10 July 2014.*

[68] ***.

75. ***. This triage process means that the vast majority (***%) of all the items collected by this process are never looked at by an analyst.[69] This figure is striking: even where communications are known to relate to specific targets, the Agencies do not have the resources to examine all of them. The number of communications collected by this process which are viewed or read by analysts amounts to *** items per day (on average).

***	Items per day
Items that match one of GCHQ's simple selectors *** and are collected and stored for possible examination.	***
Items examined by GCHQ analysts.	***[70]

***

76. In relation to the other major process we have analysed, of the approximately *** billion items per day travelling across those bearers on which it operates, GCHQ have applied selection rules and run complex searches in order to select the *** items per day most likely to be of intelligence value. These items are presented to analysts as a series of indexes in tabular form showing the results of the searches. GCHQ explained that: *"To access the full content of any of these items, the analyst then has to decide to open the specific item of interest… based on the information in the index"*.[71] In simple terms, this can be considered as similar to the search results obtained from an internet search engine (like Bing or Google) ***. Just as with a normal web search, analysts will not examine everything – they must use their judgement and experience to decide which communications appear most relevant. GCHQ explained that analysts select around *** items per day to examine: the remainder of the potentially relevant items are never opened or read by analysts.

***	Items per day
Items travelling across the chosen bearers that match one of the selection rules ***.	***
Items which match *** selected for possible examination using 'complex searches'.	***
Items that an analyst decides to examine.	***[72]

77. As a result, of the thousands of billions of communications that transit the internet every day, only around *** are examined by GCHQ analysts every day.[73] These items have been specifically selected – via a number of targeted filters and searches – as being only those that are of high intelligence value.

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

---

[69] *GCHQ have explained that intercepted content is typically stored for *** before being discarded. Related Communications Data may be stored for up to ***.*

[70] *Written Evidence – GCHQ, 10 July 2014.*

[71] *Written Evidence – GCHQ, 14 November 2014.*

[72] *Written Evidence – GCHQ, 10 July 2014.*

[73] ***.

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.**

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.

Does bulk interception work?

78. Many of the criticisms of GCHQ's bulk interception capability have focused on the allegation that there is no clear evidence that it provides valuable intelligence, or that the benefits gleaned are minimal and therefore it cannot be justified. Privacy campaigners have also highlighted examples from debates in the US regarding NSA bulk collection which they say demonstrate that bulk interception is ineffective and there is no clear advantage to be gained from it.

79. The Government has not commented on the effectiveness of bulk interception beyond broad statements that intelligence gathered through interception has contributed to preventing terrorist attacks and serious crimes. However, the Committee has questioned GCHQ in detail as to how useful bulk interception really is, and sought evidence as to how the capability has been used and why the intelligence gained could not have been gathered using any other capability.

80. We were surprised to discover that the primary value to GCHQ of bulk interception was not in reading the actual content of communications, but in the information associated with those communications. This included both Communications Data (CD) as described in RIPA (which is limited to the basic 'who, when and where' and is described in greater detail in Chapter 6), and other information derived from the content (which we refer to as Content-Derived Information, or CDI),[74] including the characteristics of the communication[75] ***. While CDI is not what might be most obviously understood to be content, under RIPA it must be treated as content, not CD. Examination of CDI therefore requires the same Ministerial authority as examination of content.

81. GCHQ have provided case studies to the Committee demonstrating the effectiveness of their bulk interception capabilities.[76] Unfortunately, these examples cannot be published, even in redacted form, without significant risk to GCHQ's capabilities, and consequential

[74] *The technical term used to describe this information is 'content-derived metadata'. However, given the confusion regarding the term 'metadata' (which we address in Chapter 6), for ease the Committee will refer to this type of information as 'Content-Derived Information' throughout.*

[75] ***.

[76] *Written Evidence – GCHQ, 27 November 2014.*

damage to the national security of the UK. We can, however, confirm that they refer to complex problems relating directly to some of the UK's highest priority intelligence requirements. (These examples are included in the classified version of the Report that is shared with the Prime Minister.)

*Example 1: ****

82. ***.

83. ***.

*Example 2: ****

84. ***.

85. ***.

86. ***.

*Example 3: ****

87. ***.

88. ***.

89. ***.

The value of bulk interception

90. The examples GCHQ have provided, together with the other evidence we have taken, have satisfied the Committee that GCHQ's bulk interception capability is used primarily to find patterns in, or characteristics of, online communications which indicate involvement in threats to national security. The people involved in these communications are sometimes already known, in which case valuable extra intelligence may be obtained (e.g. a new person in a terrorist network, a new location to be monitored, or a new selector to be targeted). In other cases, it exposes previously unknown individuals or plots that threaten our security which would not otherwise be detected.

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.

5. 'BULK' INTERCEPTION: LEGAL AUTHORITY AND PRIVACY CONCERNS

Objections to collection in principle

91. As we have noted, while communications may be collected in bulk, the examination of them is targeted according to specific criteria. Most of those who gave evidence to this Inquiry were focused on the criteria for examination of communications. However, four of the privacy campaigners who gave evidence to this Inquiry – Big Brother Watch, JUSTICE, Liberty and Rights Watch UK – told the Committee that they objected to the principle of collecting internet communications in bulk.

92. They considered that the collection of internet communications was intrusive in and of itself, even if the content of those communications was not looked at by either a computer or a person. They argued that this threatens people's fundamental rights and has a pervasive 'chilling effect' on society as a whole:

> *The objection is to both – the collection and interrogation without an appropriate framework. There is nothing passive about GCHQ collecting millions and millions of communications of people in this country… even if human beings are not processing those communications and it is being done by machines, that is a physical interception – a privacy infringement – and a model of blanket interception that we have not traditionally followed in this country.*[77]

93. We recognise their concerns as to the intrusive nature of bulk collection. However, without some form of bulk collection the Agencies would not be able to discover threats. The Courts have examined this issue – the Investigatory Powers Tribunal (IPT), ruling on RIPA Section 8(4), acknowledged *"the pre-eminent role of* [the 8(4)] *regime in the identification of threats to UK national security from abroad"*.[78] The Government has previously explained that:

> *… it would not be possible to obtain adequate levels of intelligence about individuals and organisations operating outside the British islands if interception could only be carried out in relation to communications going to or from specific addresses.*[79]

94. When we questioned the privacy campaigners who came to give evidence to this Inquiry, they made their view – that bulk interception was unacceptable – quite clear, even if that meant terrorist attacks could not be prevented:

> *HAZEL BLEARS: You are saying that bulk collection is a step too far in terms of infringement of privacy and, therefore, that if we are unable to analyse targets and develop targets in a way that, subsequently, would contribute to national security, you are prepared to forgo this possibility because of the intrusion into people's privacy. Your balance falls in not having bulk collection at all.*
>
> *ISABELLA SANKEY: Absolutely.*

---

[77] *Oral Evidence – Isabella Sankey (Liberty), 15 October 2014.*
[78] *Paragraphs 72 and 148, IPT/13/77/H, Investigatory Powers Tribunal, 5 December 2014.*
[79] *Paragraph 291.1, HMG Open Response to Case IPT/13/77/H.*

…

HAZEL BLEARS: If there were evidence that the ability to have bulk collection and then to interrogate it through targeted searches that are properly authorised under a legal framework had helped to develop targets, prevent plots and contribute to national security, would your view be different?

DR METCALFE: No.

ISABELLA SANKEY: No.

…

CHAIR: If evidence emerged through bulk interception that even you acknowledged had led to terrorists being arrested or prevented from carrying out their objectives, are you saying that, as a matter of principle, you believe so strongly that bulk interception is unacceptable in a free society that you would say that that was a price we should be willing to pay, rather than allowing intelligence agencies to use bulk interception methods?

ISABELLA SANKEY: Yes.

DR METCALFE: Yes.

…

CHAIR: And that is the view of your colleagues as well?

EMMA CARR: Yes.

…

MR HOWARTH: You object to that in principle, which is fair enough, but do you accept the corollary to that, which is that some things might happen that otherwise might have been prevented?

ISABELLA SANKEY: Yes. That is always the case in a free society. Some things might happen that could have been prevented if you took all of the most oppressive, restrictive and privacy-infringing measures. That is the price you pay to live in a free society.[80]

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.

---

[80] *Oral Evidence, 15 October 2014.*

Legal framework: 8(4) warrants and the Certificate

95. RIPA sets out that GCHQ's bulk interception is authorised by a warrant, signed by a Secretary of State, under Section 8(4). An 8(4) warrant for bulk interception is quite different from the 8(1) warrants used for targeted interception. Whereas the 8(1) warrant system provides authorisation for deliberate and specific investigation into a named individual, usually in the UK, the 8(4) warrant system is designed for much broader intelligence-gathering purposes – primarily finding threats to the UK from overseas. The Home Secretary explained to the Committee that:

> *There is a difference between the sorts of work that are done under 8(1) and 8(4)… The regimes are different because… 8(1) is an investigatory tool… whereas 8(4) is primarily an intelligence-gathering capability. So it is the case that the characteristics of what is done under the two different warrants is by nature different.*[81]

96. When considering the Regulation of Investigatory Powers Act in 2000, Parliament decided that, as a matter of principle, interception of internal communications – i.e. within the UK – should be subject to tighter controls and more rigorous safeguards than interception of external communications.

97. This position, based on principle, is strengthened by the fact that there are practical differences between gathering intelligence on individuals within the UK and gathering intelligence on those overseas. Within the UK, the Agencies and police have far greater capacity, capability and coverage, and they are therefore more likely to be able to discover threats in the first place. (For example, MI5 may be provided with leads by the public or law enforcement.)[82] As a result, it is feasible to have an interception regime which requires the threat to be known, and individual selectors to be identified, before interception takes place. However, outside the UK, the Agencies simply do not have the same resources and coverage available to discover the identity and location of individuals and organisations who pose a threat to the UK. They therefore rely on an interception regime which enables them to cast their nets wider, to discover unknown threats.

98. The 8(4) warrant which authorises this broader interception regime provides that GCHQ may intercept the external communications carried by a specific named CSP. There are 18 such warrants[83] (relating to *** CSPs), and a further one which covers GCHQ's own interception operations.[84] The warrants are valid for six months and may be renewed through a submission to the Secretary of State.

99. The purpose of the 8(4) warrants is to allow for external communications carried by that CSP to be collected by GCHQ, provided that that collection is:

i) for one or more of GCHQ's statutory purposes; and

ii) compatible with the human rights requirements of necessity and proportionality.

The warrants do not address the examination of the communications, only their collection.

---

[81] *Oral Evidence – Home Secretary, 16 October 2014.*

[82] *However, they are increasingly generating leads proactively – for example, through targeted analysis of Communications Data.*

[83] *The number of 8(4) warrants held by GCHQ changes from time to time (***). The figure of 18 was correct at the time this evidence was provided by GCHQ (12 December 2014).*

[84] *GCHQ explained that the 8(4) warrant covering their own interception ***. (Written Evidence – GCHQ, 28 February 2014.)*

100. 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 is listed in the Certificate.

8(4) WARRANTS AND CERTIFICATE

- In order to obtain an 8(4) warrant, GCHQ must put a submission to the Foreign Secretary setting out why the warrant is needed, how it will be used and the associated risks and safeguards. This is broadly the same information that is required on an application for an 8(1) warrant. We have published the information that is provided and the justification that must be made at Annex C.
- If the Foreign Secretary considers that the warrant is necessary, legal and proportionate (i.e. it meets the requirements of RIPA and of the Human Rights Act) then he will sign the warrant. The warrant itself is very brief, simply naming the CSP concerned. We have published the template for an 8(4) warrant at Annex C.
- The warrant allows the collection of communications. However, GCHQ can only examine communications where it is necessary and proportionate (in accordance with the HRA), and under authority of a Certificate. This sets out the categories of communications that GCHQ may examine: the categories directly relate to the intelligence-gathering priorities set out by the Joint Intelligence Committee and agreed by the National Security Council.

101. We have examined the Certificate and the categories of information that it sets out. We note that the categories are expressed in very general terms. For example: *"Material providing intelligence on terrorism (as defined by the Terrorism Act 2000 (as amended)), including, but not limited to, terrorist organisations, terrorists, active sympathisers, attack planning, fund-raising"*. Given that the Certificate is so generic, it begs the question as to whether it need be secret or whether, in the interests of transparency, it should be published.

102. The Certificate does not just cover national security issues: it also addresses the Agencies' other functions, i.e. safeguarding economic well-being and the prevention and detection of serious crime. It therefore includes categories such as *"controlled drugs (as defined by the Misuse of Drugs Act 1971)"*, *"***"*, *"***"*, *"***"* and *"***"*. However, we note that there is one category that did not appear directly related to any of these matters – namely *"strategic environmental issues including… ***"*. We questioned the Foreign Secretary on this point and he undertook to review both the nature and content of the 8(4) Certificate. He subsequently confirmed that the categories of information expressed in the Certificate *"closely reflect the national intelligence requirements set out by the Joint Intelligence Committee and the National Security Council"* and *"can be mapped onto the National Security Strategy's Strategic Themes"*.[85]

[85] *Written Evidence – Foreign Secretary, 5 January 2014.*

103. He explained that 'strategic environmental issues' *"*[reflect] *a legitimate UK requirement for intelligence"* and had, for example, *"allowed GCHQ to respond quickly to the Temporary Intelligence Watch in place in respect of the ***"*. ***. While this explanation was helpful, we question whether the categories could be clarified: the current Certificate appears unnecessarily ambiguous and could be misinterpreted.

104. The Foreign Secretary told the Committee that as a result of his review he had *"put in place additional oversight arrangements"* and instituted a *"formal review process to ensure that* [the] *Certificate is reviewed at least annually by the Secretary of State"*.[86]

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.

Legal framework: 'external' and 'internal' communications

105. 8(4) warrants allow GCHQ to collect 'external communications' – these are defined in RIPA as communications where at least one end is overseas.[87] Communications involving only people in the UK are classed as 'internal communications' and cannot deliberately be intercepted under an 8(4) warrant: such interception must be individually authorised by an 8(1) warrant targeted against a specific person or address, usually in the UK.

106. Twenty-five years ago it was straightforward for GCHQ to determine which communications were external and which were not. Telephone numbers would include international dialling codes and be routed through international telephone exchanges; they would self-evidently be 'external' communications.

107. However, the internet has blurred international boundaries and the distinction between 'internal' and 'external' communications travelling across the internet is not always clear. For example, an individual email address ending '.com' does not guarantee that the owner is in the USA or a US citizen, and a '.co.uk' email address could belong to a person with no connection to the UK.

108. The confusion as to what counts as an 'internal' communication or an 'external' communication is further complicated by the use of communications platforms owned and operated by providers overseas. People in the UK who use overseas email providers might only be emailing their next door neighbour, but in doing so, the communications may well travel via a computer in the USA. Such scenarios raise the question as to whether

---

[86] *The draft 'Interception of Communications Code of Practice' (published on 6 February 2015) has also clarified that "the Interception of Communications Commissioner must review any changes to the descriptions of material specified in the Certificate".*

[87] *Some communications may involve several people (e.g. a three-way video conference). These are defined as 'external communications' if at least one party to the communication is overseas.*

the nature of the internet and widespread use of internet services based overseas have rendered the distinction between 'internal' and 'external' communications meaningless.[88]

109. In order to establish how the different definitions are applied, the Committee put a number of examples to Agencies and Ministers. There seemed to be considerable confusion, even among Government, as to the different categories of communications. Giving evidence in October 2014, the Foreign Secretary considered that:

- In terms of an email, if one or both of the sender or recipient is overseas then this would be an external communication.
- In terms of browsing the internet, if an individual reads the Washington Post's website, then they have 'communicated' with a web server located overseas, and that is therefore an external communication.
- In terms of social media, if an individual posts something on Facebook, because the web server is based overseas, this would be treated as an external communication.
- In terms of cloud storage (for example, files uploaded to Dropbox), these would be treated as external communications, because they have been sent to a web server overseas.[89]

This appeared to indicate that all internet communications would be treated as 'external' communications under RIPA – apart from an increasingly tiny proportion that are between people in the UK, using devices or services based only in the UK, and which only travel across network infrastructure in the UK.

110. However, the Foreign Secretary subsequently explained:

> *When an analyst selects communications that have been intercepted under the authority of an 8(4) warrant for examination, it does not matter what form of communication an individual uses, or whether his other communications are stored on a dedicated mail server or in cloud storage physically located in the UK, the US or anywhere else (and in practice the individual user of cloud services will not know where it is stored). If he or she is known to be in the British Islands it is not permissible to search for his or her communications by use of his or her name, e-mail address or any other personal identifier...*[90]

While this appears reassuring, we note that it relies on the Agencies knowing the location of both sender and recipient which, as we have described above, may be difficult if not impossible. It appears that if both locations are unknown, then the communication may be collected as 'external', and it may be permissible for analysts to examine that communication in the belief that it relates to a person overseas.

---

[88] *Further, there is some concern that RIPA 8(4) provisions indirectly discriminate against ethnic minorities, as these communities are more likely to have relatives living overseas and are therefore more likely to have their communications intercepted. The Investigatory Powers Tribunal (IPT) considered this issue and, in a judgment of 5 December 2014, ruled that "any indirect discrimination is sufficiently justified", given the critical role of the 8(4) interception regime in identifying threats to the UK. (IPT/13/77/H, Investigatory Powers Tribunal, 5 December 2014.)*

[89] *Oral Evidence – Foreign Secretary, 23 October 2014.*

[90] *Oral Evidence – Foreign Secretary, 23 October 2014.*

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.

Legal safeguards for people in the UK

111. We were concerned that this might mean that the communications of individuals in the UK, who might have believed that their communications would always be covered by the targeted 'internal' rules (i.e. a specific 8(1) warrant), are instead covered by the less targeted 'external' rules (i.e. a broad 8(4) warrant).

112. This concern is acknowledged in RIPA. As the Foreign Secretary explained, RIPA provides different safeguards depending on whether one or both 'ends' of the communication are in the UK, and at what point the Agencies may discover this. These different circumstances are described below:

i) Where both ends of the communication are outside the UK,[91] the communication may be collected under an 8(4) warrant, may be searched for in relation to either 'end', and may be examined in accordance with the 8(4) Certificate.

ii) However, where one end of the communication is known to be in the UK, while the communication may be collected under an 8(4) warrant, the Agencies can only search for it in accordance with the 8(4) Certificate on the basis of the end that is outside the UK. On that basis, it can then be examined. For example, the Agencies are targeting Mr X, an individual known to be in Yemen. They may therefore collect, search for and examine Mr X's communications under the 8(4) warrant and Certificate, even if one email he sends goes to Mr Y, who is in the UK. What the Agencies cannot do under the 8(4) regime is search for and examine Mr Y's communications.

iii) Where one end of the communication is known to be in the UK, if the Agencies wish to search for it on the basis of that end (i.e. Mr Y's communication), then they cannot do so under the broad 'external' 8(4) regime. RIPA requires that searching for the communications of an individual in the UK requires a more specific and targeted authorisation, signed by a Secretary of State. This can either be in the form of a targeted 8(1) interception warrant, or a 'top-up' of the 8(4) warrant called a Section 16(3) modification. (A Section 16(3) modification provides the Agencies with a similar authority to an 8(1) warrant – we discuss 16(3) modifications in more detail below.) In other words, while GCHQ might have incidentally collected the communication of a person in the UK under 'external rules', they can only search for that communication (and then examine it) under 'internal rules'. Using the previous example, if the Agencies wish to search for Mr Y's communications amongst all the communications they have collected, then because they know he is in the UK they must apply either for an 8(1) warrant or a 16(3) modification – an 8(4) warrant is not sufficient.

[91] *Or, in the case of communication involving more than two individuals, all ends are outside the UK.*

iv) Occasionally, the Agencies search for a communication on the basis of the end that is outside the UK (as in (ii) above), but when they examine it they discover that it belongs to a person in the UK. (As we have explained previously, the nature of the internet – where individuals communicating have no verified identity or location – means that this cannot be avoided in all circumstances.) In these circumstances, the analyst must stop searching for and examining the communications of that person. If the Agencies wish to continue searching for and examining that individual's communications (as set out above), they must first seek either an 8(1) warrant or a 16(3) modification.[92] Using the example given previously, the Agencies consider that Mr X is in Yemen, and search for his communications in accordance with the 8(4) regime. However, when they examine a communication they realise that Mr X is actually in the UK. The Agencies must cease all action at that point, until they have obtained separate authority from a Secretary of State under the 'internal rules' (i.e. an 8(1) warrant or a 16(3) modification).

v) On occasion, the Agencies may discover, upon examining a communication, that both ends of the communication are in the UK – i.e. it is a UK-to-UK communication.[93] In such circumstances they cannot continue to search for or examine communications between those two individuals under the 8(4) regime, and they cannot use the 16(3) modification. They must instead apply for an 8(1) warrant. Examination of all UK-to-UK communications must be covered by a specific, named authorisation.

Section 16(3) modifications

113. Given the importance of this form of additional Ministerial authorisation in relation to individuals in the UK, we questioned the Foreign Secretary about the nature of the application process. He told us that the 16(3) modification process is as rigorous as an 8(1) warrant process – the same level of rationale and justification is required, and the same legal tests are applied.

114. The examples of 16(3) modifications we have seen show that the information provided to the Foreign Secretary is detailed and addresses why the interception is necessary and proportionate. However, these modifications do not cover all the categories of information that an 8(1) application would cover (for example, any expected collateral intrusion into the privacy of others, or why the intelligence sought cannot be obtained by less intrusive means). Furthermore, GCHQ noted that 16(3) modifications may contain lists of individuals – i.e. they do not always relate to a specific individual in the same way as 8(1) warrants.[94]

115. We questioned GCHQ as to why the 16(3) modification exists, and why they do not apply for an 8(1) warrant whenever they become aware that they are targeting a person in the UK. GCHQ said that this would have *"a significant operational impact*

---

[92] *The law recognises that a target being investigated as a potential risk to national security does not cease to be a risk simply because they have travelled to the UK, or have been discovered to be already located within the UK. It therefore allows for a temporary (internal) authorisation from senior managers to continue examining the intercepted communications for up to five working days. This takes the form of a Section 16(5) authorisation and is designed to allow time for further analysis of the target's location (i.e. to establish whether they are definitely in the UK or not) and time to seek the greater and more targeted authority of a 16(3) modification or 8(1) warrant from a Secretary of State (where it is established that the individual is in the UK and it is necessary and proportionate to seek to examine their communications).*

[93] *This may happen either when the Agencies search for a communication on the basis of the end that is outside the UK, but then they discover that that end is actually in the UK, and that the communication is to another person in the UK, or when the Agencies search for a communication of a person known to be in the UK and discover that it is to another person in the UK.*

[94] *In exceptional circumstances, a Secretary of State may approve a 'thematic' 8(1) warrant as described in paragraphs 42–45.*

for GCHQ and resourcing consequences for both GCHQ and [the Foreign Office and Northern Ireland Office]*"*, given the *"resulting increase in applications/renewals (with additional administrative load and abstraction of operational staff to handle it)"*, which would result in a *"loss of operational flexibility and timeliness, through the need to list every wanted selector on an 8(1) warrant schedule, and to submit schedule modifications each time it was necessary to add or remove a selector"*.[95]

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.

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.

Additional protection for UK nationals overseas

116. The RIPA warrant regime is based on geography, rather than nationality. Therefore, while it provides additional safeguards for individuals in the UK, it does not do so for UK nationals overseas. However, GCHQ recognise the particular sensitivities around the targeting of UK nationals, and this policy position is reflected in their operational approach: GCHQ have implemented an additional system of internal authorisations for the communications of UK nationals overseas to provide that further assurance. ***.[96]

---

[95] *During 2013 GCHQ obtained *** RIPA 16(3) modifications from a Secretary of State. (Written Evidence – GCHQ, 4 December 2014 and 31 December 2014.)*

[96] ***.

117. This is not a formal, legal requirement (unlike a RIPA 16(3) modification relating to communications of people in the UK). However, it does mean that there is a further consideration of necessity and proportionality before such communications can be examined.[97, 98]

118. We have questioned whether British citizens, irrespective of their location, should be afforded the same level of protection – i.e. that a Secretary of State must authorise the interception and examination of their communications on a case-by-case basis. In practice, this would mean requiring GCHQ to seek an 8(1) warrant in every case.

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.

Storage and security

119. Some contributors to this Inquiry raised concerns as to how the information collected by GCHQ was stored, in particular:

- the length of time that GCHQ store information obtained from bulk interception; and
- the security of GCHQ's data stores (either in terms of leaking, misuse by a disgruntled employee or the possibility that they could be hacked into by a third party).

120. In terms of the retention of data and communications collected by GCHQ, there are several stages of GCHQ's bulk interception capability which involve storage. In general terms, the earlier stages of this capability involve greater volumes of communications retained for very short periods of time (e.g. accessing communications bearers to determine those most likely to be carrying communications relevant to GCHQ's work). Communications being accessed during later stages of the *** process are *** compared against GCHQ's list of targets – any that match are stored for up to *** (or longer in some limited circumstances).[99]

121. ***. Any communications which match one of the complex searches GCHQ carry out are available for an analyst to examine. Only those that the analyst considers are of legitimate intelligence value are copied *** into longer-term storage – again these are held for up to *** (or longer in some limited circumstances).[100]

---

97 ***.

98 *Written Evidence – GCHQ, 10 July 2014.*

99 *GCHQ's standard policy is to retain the content of selected communications for *** and the Related Communications Data for up to ***. However, in some circumstances (such as voice communications where a transcript has been produced from the recording) the content or RCD may be held for up to ***.*

100 *Written Evidence – GCHQ, 28 February 2014.*

122. In terms of protecting the data and communications that they do hold, GCHQ explained that they go to great lengths to protect the information held on their systems – one of GCHQ's primary roles is to provide advice and assistance to the Government and the private sector on the security of communications and electronic data and therefore they take their own responsibilities very seriously. Following the actions of Edward Snowden, GCHQ took a variety of steps to reduce their 'information risk', including increased logging and auditing and a full review of access to their key systems.[101]

Oversight and audit

123. As we have explained, the 8(4) Certificate sets out the general categories of information which may be examined. In practice, it is the selection of the bearers, the application of simple selectors and initial search criteria, and then complex searches which determine what communications are examined. It is therefore these that are of most importance. As a result, the Committee has sought assurances that they are subject to scrutiny and review by Ministers and/or the Commissioners.

124. However, from the evidence we have taken, it appears that neither Ministers nor the Commissioners have any significant visibility of these issues. (For example, neither were aware that the number of 'selection rules' *** had doubled between March and November 2014.) The Government considered that GCHQ had been given legal authority to collect and examine certain communications, and Ministerial tasking through the National Security Council, and therefore the Foreign Secretary would not approve the individual selection rules.

125. While we recognise this argument in relation to Ministers – they have already provided authority – we nevertheless consider that the retrospective review or audit of these criteria is essential.

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.

126. Bulk interception techniques access internet communications on a large scale, even if it is only a small proportion of the total, and then collect a reservoir of data that analysts may search within. However, analysts are not permitted to trawl through the held data on 'fishing expeditions': this would be unlawful. For a public servant it could constitute misconduct in public office (a criminal offence), or for others, such as contractors, they would be liable in the civil courts.

127. In simple terms, material that is collected under an 8(4) warrant may be examined, read or analysed only if:

- it is for one of the Agencies' statutory purposes (i.e. safeguarding national security, including where this relates to the economic well-being of the UK, or for the prevention and detection of serious crime);

[101] *Written Evidence – GCHQ, 3 February 2014.*

- it is necessary, in that the information being sought cannot be obtained through other less intrusive means;
- it is proportionate, meaning that the intrusion must be justified for the purpose of the investigation and must include consideration of the impact it may have on the privacy of innocent people; and
- it relates to a category of information that is specified in the accompanying Certificate – anything that is not within the terms of the Certificate may be intercepted but may not be read, looked at or listened to by any person.

128. We have examined what safeguards there are to ensure that staff do not search for or examine material not covered by these criteria. GCHQ explained to the Committee that:

- every search of, or query against, the stored information has to be clearly linked to one of their statutory purposes (as set out in the Intelligence Services Act 1994) and to a valid UK intelligence requirement, and justified as being necessary and proportionate;
- GCHQ systems generate logs which are automatically passed to the Information Security team for audit: *"Automated rules, designed to identify indicators of the most likely types of unauthorised use, are run against the logs, and any anomalies are investigated"*.[102] The justification for the search is also subject to an audit programme – samples of justifications are audited by operations teams and an HRA Auditing Steering Group;
- deliberate abuse of access to GCHQ's systems would constitute gross misconduct (depending on the circumstances) – to date there has only been one case where GCHQ have dismissed a member of staff for misusing access to GCHQ's systems; and
- the Interception of Communications Commissioner is provided during his inspection with the results of any audits conducted.

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.

[102] *Written Evidence – GCHQ, 10 April 2014.*

6. COMMUNICATIONS DATA

- ➢ Communications Data (CD) means the details about a communication (the 'who, when and where') but not the content of what was said or written.
- ➢ The types of CD are defined in Chapter II of RIPA Part I and in the RIPA '*Code of Practice on the Acquisition and Disclosure of CD*', 2007.

129. The Committee provided a detailed explanation and examples of CD in its Report '*Access to communications data by the intelligence and security Agencies*', dated February 2013:

> *CD is the information created when a communication takes place – for example, the time and duration of the contact, telephone numbers or email addresses, and sometimes the location of the device from which the communication was made. More detailed examples are as follows:*
>
> - *Landline telephones: details about numbers dialled by a telephone; time/dates calls are made and received; name and address details of the person who pays the line rental.*
> - *Mobile telephones: as above, but also the approximate location from which a call/text was made or received by a handset.*
> - *Internet telephony: the online username, login name or account name from which a call is made or received; the date/time of the call; and the internet addresses (IP addresses) of the computers used.*
> - *Email: the email addresses of the sender and recipient; the date/time of the message; and the internet addresses (IP addresses) of the computers used.*
> - *Instant/social messaging: the online user, login name or account name from which a message is sent or received; the date/time the message was sent; and the internet addresses (IP addresses) of the computers used.*
> - *Web browsing: the IP address of the device being used to access the Internet; time and date of logon and logoff; record of web domains visited.*

Why do the Agencies need access to CD?

130. CD 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 (through the use of subscriber checks) and to illuminate networks and associations relatively quickly.[103] It can be particularly useful in the early stages, when the Agencies have to be able to determine whether those associating with the target are connected to the plot (and therefore require further investigation) or are innocent bystanders. GCHQ have established that they can analyse CD to find patterns in it that reflect particular online behaviours that are associated with activities such as attack planning, and to establish links. (***.) The Committee has seen – from its investigation in

[103] *CD is also an important tool for SIS ***.*

2008 into Operation CREVICE – how valuable CD can be.[104] During the most intensive part of this operation, MI5 analysed more than 4,000 telephone contacts to establish the full extent of the terrorist network.

131. The Government and the Agencies have explained to the Committee the need for access to CD, and the extent to which it has contributed to operations. The Home Secretary has stated that *"Communications data has played a significant role in every Security Service counter-terrorism operation over the last decade"*.[105] The Director General of MI5 has explained that *"comms data is very often one of the early means we can use to determine whether and where to focus our investigation"*.[106]

132. In our 2013 Report, we said that *"it is clear to us from the evidence we have been given that CD is integral to the work of the… Agencies"*, that it is the *"easiest, and least intrusive, way"* to determine whether those associated with the target are connected to the plot and that the Agencies would have to use more intrusive capabilities if CD was not available.

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.

What categories of CD do the Agencies collect?

133. The Agencies collect the following three categories of CD:

- traffic data – information attached to, or comprised in, the communication which tells you something about how the information is sent (e.g. an address or routing information). It includes caller line identity, dialled number identity, cell location data, and other details of the location or 'address' (whether postal address or electronic address) of a sender or recipient of a communication;
- service use information – this includes billing and other types of service use information such as call waiting and barring, redirection services and records of postal items; and
- subscriber information – includes any information (that is not traffic data or service use information) that is held by the CSP 'in connection with' the provision of the service. This could include the name and address of the subscriber, bank details and details of credit cards etc. attached to a user's account.

How do the Agencies collect CD?

134. The Agencies collect CD either directly from CSPs, from their own interception of traffic (running over fibre optic cables or via satellites and other more traditional forms of communication), or from overseas partners:

i) **Targeted requests to CSPs:** these relate to a specific individual or an individual's user or service account.

---

[104] *This was an investigation into a group of terrorists who were plotting to detonate a fertiliser bomb in the UK in 2004.*
[105] *Home Secretary's oral statement to the House of Commons about the use of communications data and interception, 10 July 2014.*
[106] *Oral Evidence – MI5, 8 May 2014.*

- Authorisation and oversight: Section 22 of RIPA, authorised internally within the Agencies,[107] reviewed by the Interception of Communications Commissioner.
- Category of data: traffic data, service use information and subscriber information.
- Volume: during 2013, the Agencies submitted a total of 58,996 notices or authorisations for CD to CSPs[108] (MI5 submitted 56,918, GCHQ submitted 1,406 and SIS submitted 672).[109]
- Retention: MI5's maximum retention period is *** and GCHQ's is ***.[110]

ii) ***.

- ***.[111, 112]
- ***.[113]
- ***.[114]
- ***.[115]

iii) **Related CD (RCD) from interception:** GCHQ's principal source of CD is as a by-product of their interception activities, i.e. when GCHQ intercept a bearer, they extract all CD from that bearer. This is known as 'Related CD'. GCHQ extract all the RCD from all the bearers they access through their bulk interception capabilities (as covered in the previous chapter).

- Authorisation and oversight: already covered by an 8(1) or 8(4) interception warrant under RIPA, overseen by the Interception of Communications Commissioner.
- Category of data: traffic data.
- Volume: during 2013, GCHQ collected RCD from approximately *** communications per day from interception.[116]
- Retention: maximum of ***.

iv) **RCD from Signals Intercept:** GCHQ use their own SIGINT capability to collect CD ***.

---

[107] *Either at the equivalent of Police Inspector level (for subscriber information) or at the equivalent of Superintendent level (for service use and traffic data).*

[108] *An application for CD from a CSP requires a senior official to give notice or grant an authorisation. If a CSP has a secure auditable disclosure system, then an authorisation is used to acquire the CD; if not, a notice is served.*

[109] *'2013 Annual Report', Interception of Communications Commissioner, 8 April 2014. Each request may result in a number of individual items of CD. We asked the Agencies how many individual items their 2013 requests resulted in; however, they were unable to provide a figure. The Interception of Communications Commissioner said in his Report that the Code of Practice should require public authorities to record and report the number of individual items of CD requested rather than just the number of authorisations and notices.*

[110] *This is a longer period than for other access to CD, reflecting the fact that CD from targeted requests is, by its nature, selective.*

[111] ***.

[112] ***.

[113] ***.

[114] ***.

[115] ***.

[116] *Written Evidence – GCHQ, 14 and 24 November 2014. The vast majority of RCD is collected as a result of GCHQ's bulk interception of external communications. A small proportion will result from 8(1) interception of UK communications.*

- Authorisation and oversight: collection from communications systems which fall under RIPA is authorised by an 8(4) warrant signed by a Secretary of State and overseen by the Interception of Communications Commissioner; CD collection from other systems under the Wireless Telegraphy Act 2006 is authorised by a Secretary of State. There is no oversight of interception carried out under the Wireless Telegraphy Act.[117]
- Category of data: traffic data.
- Volume: during 2013, GCHQ collected RCD from signals intercept relating to approximately *** communications per day.[118]
- Retention: maximum of ***.

v) **Overseas partners:** GCHQ can receive CD from their overseas partners. This is primarily as a by-product of requests for targeted interception material. However, there are two ways they obtain CD in bulk, albeit on a small scale: ***.[119]

- Authorisation and oversight: through the 'gateway' provisions of the Intelligence Services Act 1994 (see Chapter 10). These arrangements are not subject to formal oversight by the Commissioners.
- Category of data: traffic data.
- Volume: from bulk interception, ***.[120] (No figures available for targeted requests.)
- Retention: maximum of ***.

Key issues

135. Those who submitted evidence to this Inquiry raised several concerns in relation to CD and we have ourselves identified further concerns. The three key issues are:

a) whether CD is now as intrusive as content;

b) the acquisition of UK-to-UK RCD; and

c) ***.

a) Is CD as intrusive as content?

136. RIPA defines CD as the basic 'who, when and where' of a communication. It does not define any other categories of information – everything other than CD is taken to be content. However, the Committee has heard arguments that this distinction is no longer meaningful. The Chair of the Equality and Human Rights Commission, Baroness O'Neill, told the Committee that the distinction was now *"technologically obsolete"*.[121] The Shadow Home Secretary, the Rt. Hon. Yvette Cooper, MP, told the Committee: *"We have… had stronger safeguards around intercept, compared to communications data. However, those distinctions now seem to be much more blurred*

[117] *We address the requirement for oversight of GCHQ's use of the Wireless Telegraphy Act 2006 in Chapter 10.*
[118] *Written Evidence – GCHQ, 14 and 24 November 2014.*
[119] *Such exchanges are often reciprocal in nature: ***.*
[120] *Written Evidence – GCHQ, 2 December 2014.*
[121] *Oral Evidence – Baroness O'Neill, 14 October 2014.*

and difficult to sustain… I think the relationship between Communications Data and content needs to be looked at again".[122]

137. Others who provided evidence to this Inquiry considered that the problem arose not from a blurring of boundaries, but due to the increased volume of communications that are now generated by individuals in their everyday lives, and the increased ability of the Agencies to collect and process these communications more quickly and on more people. It is suggested that if an Agency has the 'who, when and where' (i.e. CD) of the 100 emails, 50 internet pages and 20 text messages that an individual might now send or browse in one day, then this volume, when combined, gives the Agency a much 'richer' picture than the 'who, when and where' of the 10 phone calls and one letter an individual might have sent 25 years ago.[123]

138. In its submission to this Inquiry, Amnesty International said: *"when accessed and analysed, Communications* [Data]*... can still create a profile of an individual's life, disclosing as much as would be discernible from the content of communications"*.[124] This impact is exacerbated by the greater expectation of anonymity when using the internet. For instance, an individual seeking help with an embarrassing medical problem is more likely initially to research it on the internet – as they expect this to be private and anonymous – rather than making a telephone call to speak to someone about it.

139. We put these concerns to Ministers and Agencies. However, the Government did not consider that there had been any significant change. The Home Secretary told the Committee:

> *I do not think we have reached the point at which you can say that data is now so close to content that you have to have the same process for both of these. I think they are still distinct.*[125]

In terms of volume, she said that she did not think that that required *"in itself, a different approach to be taken"*.

140. The Agencies supported this position: in their view it remains substantively more intrusive to read the content of an email or to listen to the phone calls of a suspect than to analyse CD. The Director General of MI5 explained:

> *The suggestion that, by knowing which websites people have visited, that that is some substantial step up in intrusion, is not one I accept. Life is different these days. But browsing through different websites, much like browsing telephone calls made and where people go in their daily lives along the street, I am not sure these things are substantially different. What is transacted in the content would require an intrusive warrant.*[126]

Indeed, the Agencies maintain that analysis of CD helps to reduce intrusion (including any collateral intrusion) by improving the targeting of more intrusive capabilities.

---

[122] *Oral Evidence – Rt. Hon. Yvette Cooper, MP, 15 October 2014.*
[123] *There is also the ability to locate and track individuals via mobile phones – a capability that was not available 25 years ago.*
[124] *Written Evidence – Amnesty International, 7 February 2014.*
[125] *Oral Evidence – Home Secretary, 15 October 2014.*
[126] *Oral Evidence – Director General MI5, 8 May 2014.*

Confusion over definitions

141. A further complicating factor in this debate is the confusion as to what is treated as CD and what is treated as content. The confusion is caused, in part, by many commentators using the term 'metadata' for information that does not appear to fall neatly into either category. 'Metadata' is a term commonly used in the USA, but it has no legal definition in RIPA and therefore no bearing on the UK system of interception. For example, in the UK a record of a website visited (e.g. http://www.google.com) is treated as CD, whereas the full web address, which includes the precise words searched for (e.g. http://www.google.co.uk/search?q=ISC), is treated as content. Both of these, however, might be referred to as 'metadata'. This Committee has previously noted this confusion, particularly in relation to internet communications and web browsing histories, and has already recommended greater clarity and transparency around the different categories of information.[127]

142. During this Inquiry, it has become apparent that it may be helpful to consider communications in terms of the following four categories (these are defined by the Committee – they are not the categories recognised by RIPA):

Type of information	**Example (in relation to a telephone call)**
Communications Data	The numbers and date/time of a telephone call.
'Communications Data Plus'	Details of the person or organisation called, which could reveal details about a person's private life (e.g. if it was a call to a particular medical helpline, or a certain type of dating or sex chat line).
Content-Derived Information	The accent of an individual speaking during the call.
Content	What was said during the call.

143. While the definitions of basic CD and content above are no different from the existing arrangements under RIPA, our definitions introduce two new categories of information relating to a communication:

i) 'Communications Data Plus' – this goes further than the basic 'who, when and where' of CD. So, for example, this would encompass details of web domains visited or the locational tracking information in a smartphone. Under RIPA, the majority of this information is currently treated as CD (the acquisition of which is governed on the basis of it being relatively unobtrusive), although some is treated as content (e.g. full web browsing histories).

ii) 'Content-Derived Information' – this is information which the Agencies can only obtain by processing or analysing the content of a communication (for example, the accent of the person speaking, but not what they actually say). This is – correctly – treated as content in RIPA, even though it is not the actual content of the communication (while clearly separating this category from content, we are not proposing that it should be treated differently).

[127] *'Access to communications data by the intelligence and security Agencies', Intelligence and Security Committee of Parliament, February 2013.*

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.

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.

b) Filtering out UK-to-UK Related Communications Data

144. As described in the previous chapter, GCHQ target those bearers most likely to contain external communications, and this minimises the unintended interception of UK-to-UK communications. However, GCHQ have explained that while they do not seek to collect UK-to-UK communications, they cannot avoid incidentally intercepting some because the origin of the sender or recipient is not always clear from the CD – for example, if they had an email address ending with @gmail.com or @hotmail.com. (The only way GCHQ could be confident of filtering out UK-to-UK communications would be to examine all of it.) RIPA recognises that it is not possible to filter out all UK-to-UK communications and therefore allows for incidental interception.[128]

145. Where GCHQ do incidentally collect a UK-to-UK communication, they cannot examine the content of that communication without an additional Ministerial Authorisation, in the form of a 16(3) modification. (If they wished to search for any further communications between those two individuals in the UK, this would require an 8(1) warrant – as we set out in paragraph 112(v).) However, this safeguard does not apply to the Related Communications Data (RCD) of those communications.

146. In other words, while the content of UK-to-UK communications incidentally collected by GCHQ attracts special protection and additional safeguards under RIPA, these do not apply to the CD related to those communications. This means that UK-to-UK RCD will be in the pool of Communications Data that GCHQ collect, and may be returned as a result of searches against that pool.

*c) ****

147. ***.

148. ***.[129]

149. ***.[130]

---

[128] ***.

[129] *Written Evidence – GCHQ, 28 February 2014.*

[130] ***.

***

***

- ***;
- ***;
- ***;
- ***; and
- ***.[131]

***.

150. ***.

[131] *Written Evidence – GCHQ, 10 July 2014.*

7. BULK PERSONAL DATASETS

➢ Bulk Personal Datasets are large databases containing personal information about a wide range of people. The Agencies use these datasets in three ways:

a. to help identify SoIs, or unknown individuals who surface in the course of investigations;

b. to establish links between individuals and groups, or else improve understanding of a target's behaviour and connections; and

c. as a means of verifying information that was obtained through other sources (such as agents).

151. In addition to obtaining intelligence through capabilities such as interception, the Agencies also acquire Bulk Personal Datasets containing personal information about a large number of people. Bulk Personal Datasets may relate to the following types of information:

i) ***;

ii) ***;

iii) ***;

iv) ***;[132] or

v) ***.[133]

The Committee has examined the lists of Bulk Personal Datasets that the Agencies can access: we consider that they are relevant to national security investigations.

152. SIS explained that Bulk Personal Datasets:

> *... are increasingly used to identify the people that we believe that we have an interest in; and also to identify the linkages between those individuals and the UK that we might be able to exploit.* ***.[134]

***.[135, 136]

153. GCHQ have told us that they consider Bulk Personal Datasets to be an increasingly important investigative tool, which they use primarily to 'enrich' information that has been obtained through other techniques:

***.[137]

---

[132] ***.

[133] *Written Evidence – GCHQ, 10 July 2014; MI5, 22 August 2014; SIS, 3 October 2014.*

[134] *Oral Evidence – SIS, 15 May 2014.*

[135] ***.

[136] *Oral Evidence – SIS, 15 May 2014.*

[137] *Written Evidence – GCHQ, 28 February 2014.*

154. Bulk Personal Datasets may be acquired through overt and covert channels. The Agencies' current holdings include: ***.[138]

155. The number of Bulk Personal Datasets that each Agency holds fluctuates over time as they acquire new datasets, and they have told us that those which have not proven to be of intelligence value are deleted. As of mid-2014:

- SIS held *** Bulk Personal Datasets;
- MI5 held ***; and
- GCHQ held ***.[139]

The Committee was told that the Agencies may share Bulk Personal Datasets between them where they consider this to be lawful, necessary and proportionate.

156. These datasets vary in size from hundreds to millions of records. Where possible, Bulk Personal Datasets may be linked together so that analysts can quickly find all the information linked to a selector (e.g. a telephone number or ***) from one search query. ***.[140]

Authorisation

157. Whereas the Agencies' capabilities to intercept communications and acquire Communications Data are regulated by RIPA, the rules governing the use of Bulk Personal Datasets are not defined in legislation. Instead, the Agencies derive the authority to acquire and use Bulk Personal Datasets from the general powers to obtain and disclose information (in support of their organisation's functions) that are afforded to the heads of each of the Agencies under the Intelligence Services Act 1994 and the Security Service Act 1989.[141] (These general powers are considered in detail in Chapter 10.)

158. The Committee has a number of concerns in this respect:

- Until the publication of this Report, the capability was not publicly acknowledged, and there had been no public or Parliamentary consideration of the related privacy considerations and safeguards.
- The legislation does not set out any restrictions on the acquisition, storage, retention, sharing and destruction of Bulk Personal Datasets, and no legal penalties exist for misuse of this information.

---

[138] *The Director General of MI5 has explained that "in 2008, the Government deliberately… added Section 19 of the Counter-Terrorism Act [2008], which is an explicit licensing to those who might share data, that doing so overrides any other duties of confidentiality they might have about data, where a case is made that it is necessary to share that for national security". (Oral Evidence – MI5, 8 May 2014.)*

[139] *Written Evidence – GCHQ, 10 July 2014; MI5, 22 August 2014; SIS, 3 October 2014. ***.*

[140] *Written Evidence – SIS, 5 March 2014.*

[141] *Section 4(2)(a) of the Intelligence Services Act 1994 (ISA) imposes a duty on the Director of GCHQ to ensure "that there are arrangements for securing that no information is obtained by GCHQ except so far as necessary for the proper discharge of its functions and that no information is disclosed by it except so far as necessary for that purpose". Similar duties are imposed on the Chief of the Secret Intelligence Service (SIS) by Section 2(2)(a) of ISA, and on the Director General of MI5 by Section 2(2)(a) of the Security Service Act 1989.*

- Access to the datasets – which may include significant quantities of personal information about British citizens[142] – is authorised internally within the Agencies without Ministerial approval.

159. While Ministers are not required to authorise the acquisition or use of Bulk Personal Datasets in any way, the Home Secretary explained that she had some involvement: *"*[MI5] *do come to me and I receive submissions on acquisition of bulk datasets and the holding of bulk datasets"*.[143] In relation to the Bulk Personal Datasets held by GCHQ and SIS, the Foreign Secretary explained to the Committee that: *"There's not a formal process by which we've looked* [at those datasets]*"*. However, this is an area which he is currently reviewing. He explained:

> [I am] *often, but not always, consulted before acquisition of new datasets… I was consulted recently on a specific acquisition of a dataset that has been made. Following that, I asked for a report from SIS, which I've had, about their holdings and the handling arrangements, following which I asked to make a visit for a discussion about this and an understanding of how it works in practice… I have also asked for twice yearly reporting of the holdings of bulk personal data by the agencies.*[144]

160. In terms of independent review, the Intelligence Services Commissioner has non-statutory responsibility for overseeing the Agencies' holdings of Bulk Personal Datasets (since 2010). He told the Committee that:

> *It's actually outside the statute, but my oversight of bulk data in one sense is very formal… I didn't want there to be any misunderstanding about that. But I would prefer it to be on a statutory basis myself.*[145]

The Commissioner explained to the Committee that he retrospectively reviews the Agencies' holdings of Bulk Personal Datasets as part of his six-monthly inspection visits. This includes reviewing the intelligence case for holding specific datasets, necessity and proportionality considerations, the possible misuse of data and how that is prevented. The Intelligence Services Commissioner considers this last aspect to be of primary importance, in that: *"… it is critical that access to bulk data is properly controlled and it is the risk that some individuals will misuse the powers of access to private data which must be most carefully guarded against"*.[146]

Internal controls

161. The Agencies have told the Committee that the acquisition and use of Bulk Personal Datasets is tightly controlled, and that the HRA 'triple test' (i.e. for a lawful purpose, necessary and proportionate) is considered both at the point of acquisition, and also before any specific searches are conducted against the data (which is when they consider the principal intrusion into an individual's privacy to occur).

---

[142] *None of the Agencies was able to provide statistics about the volume of personal information about British citizens that was included in these datasets.*

[143] *Oral Evidence – Home Secretary, 16 October 2014.*

[144] *Oral Evidence – Foreign Secretary, 23 October 2014.*

[145] *Oral Evidence – Sir Mark Waller, 30 October 2014.*

[146] *Written Evidence – Sir Mark Waller, 4 February 2015.*

162. Senior staff are responsible for authorising the acquisition of Bulk Personal Datasets.[147] The Director General of MI5 explained:

> *... there are datasets that we deliberately choose not to reach for, because we are not satisfied that there is a case to do it, in terms of necessity and proportionality;* ***.[148]

The Agencies each have a review panel, chaired by a senior official, which meets every six months to review the Bulk Personal Datasets currently held by the Agency. Within MI5, each Bulk Personal Dataset has a different review period, depending on the level of intrusion and corporate risk it carries. Datasets that are found not to have sufficient operational value are deleted.[149]

163. The Agencies have said that they apply strict policy and process safeguards to control and regulate access to the datasets. The Director General of MI5 explained:

> *... we only access this stuff... where there is an intelligence reason to do it. So we start off with a threat, a problem, a lead, that then needs to be examined and pursued and either dismissed or lead to action to counter it. That is when we use the data. It is absolutely not the case that there is anybody in MI5 sat there, just trawling through this stuff, looking at something that looks interesting; absolutely not.*[150]

These controls include:

i) Training, audit and disciplinary procedures

All staff with access to Bulk Personal Datasets are trained on their legal responsibilities; all searches must be justified on the basis of necessity and proportionality; and all searches may be audited to ensure that any misuse is identified. Each Agency reported that they had disciplined – or in some cases dismissed – staff for inappropriately accessing personal information held in these datasets in recent years.[151]

ii) Heightened safeguards for sensitive categories of information

The Agencies may use stronger controls around access to certain sensitive information. Depending on the context,[152] this may include, but is not limited to, personal information such as an individual's religion, racial or ethnic origin, political views, medical condition, ***, sexual orientation, or any legally privileged, journalistic or otherwise confidential information.

We note that while these controls apply inside the Agencies, they do not apply to overseas partners with whom the Agencies may share the datasets. (The sharing of intelligence is considered in Chapter 10.)

---

147 ***.

148 *Oral Evidence – MI5, 8 May 2014. ***.*

149 *'High risk' Bulk Personal Datasets are reviewed every six months; 'medium risk' Bulk Personal Datasets are reviewed every 12 months; and 'low risk' Bulk Personal Datasets are reviewed every two years.*

150 *Oral Evidence – MI5, 8 May 2014.*

151 ***.

152 *For example, the religion of an SoI may be important in the context of tribal politics in Iraq, and therefore retained in a Bulk Personal Dataset, whereas religion may be irrelevant in other contexts and therefore deleted from the dataset.*

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.

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.

8. OTHER AGENCY CAPABILITIES

- ➢ The privacy debate has largely focused on the Agencies' ability to intercept communications and acquire Communications Data. However, the Agencies have a number of other intrusive capabilities.
- ➢ These include:
  - Surveillance;
  - Interference with Property (including IT Operations);
  - Interference with Wireless Telegraphy;
  - Reading Encrypted Communications; and
  - Covert Human Intelligence Sources.
- ➢ These capabilities are regulated under either the Intelligence Services Act 1994 or the Regulation of Investigatory Powers Act 2000.

a) Surveillance

164. Surveillance – which can be either 'Intrusive' or 'Directed' – is defined by the RIPA '*Covert Surveillance and Property Interference Code of Practice*' as:

> *… monitoring, observing or listening to persons, their movements, conversations or other activities and communications. It may be conducted with or without the assistance of a surveillance device and includes the recording of information obtained.*[153]

'Intrusive Surveillance'

165. 'Intrusive Surveillance' refers to the use of covert techniques to monitor an SoI's movements, conversations and activities in private places where there would be a heightened expectation of privacy, such as inside a suspect's home or vehicle.[154] This capability is highly intrusive as it involves observation of the private life of SoIs, their families and their close associates. It is therefore used sparingly and is normally deployed in support of only the highest priority investigations.

166. Intrusive Surveillance is authorised by a warrant signed by a Secretary of State. This can either take the form of an Intrusive Surveillance Warrant under the Regulation of Investigatory Powers Act 2000 (RIPA), or a warrant combining both the Intrusive Surveillance Authorisation under RIPA and the 'Interference with Property' Authorisation under the Intelligence Services Act 1994 (ISA) (a 'Property and Intrusive Surveillance

[153] *'Covert Surveillance and Property Interference Code of Practice', 10 December 2014.*

[154] *This includes any place where a person may be expected to take legal advice. It does not include taxis or communal or non-residential areas of a hotel or a prison as these are considered to be public environments.*

Warrant', PSW).[155] Both warrants are valid for six months – unless cancelled or extended with prior agreement from a Secretary of State. However, the Committee has been told that, in some long-standing cases, PSWs have been in place for several years (albeit renewed by the Home Secretary every six months). The Intelligence Services Commissioner has statutory responsibility under RIPA for retrospective review of these warrants.

167. The Committee asked the Agencies how frequently they had used this capability within the UK. They told us that during 2013 a total of *** authorisations were obtained. Of these:

- all of the combined Property and Intrusive Surveillance Warrants (***) were obtained by MI5, together with around a third of the Intrusive Surveillance Warrants (***);
- SIS obtained the remaining two-thirds of the Intrusive Surveillance Warrants (***) *"to authorise activity against a mixture of individuals and groups (***)… we estimate *** individuals were targeted"*;[156] and
- GCHQ obtained a very small proportion of these authorisations (***, in the form of combined ISA Section 5 Warrants and RIPA authorisations for Intrusive and Directed Surveillance), to allow them to ***.[157]

168. Outside the UK, the Agencies undertake Intrusive Surveillance on the basis of an authorisation from the Secretary of State under Section 7 of ISA. (This removes criminal and civil liability for classes of activity – such as Intrusive Surveillance – undertaken outside the British Islands which would otherwise be offences under UK law. ISA Class Authorisations are covered in more detail in Chapter 10.) However, there are no figures for the use of this capability outside the UK because it is conducted under a Class Authorisation, and the numbers of operations are not recorded centrally.

'Directed Surveillance'

169. 'Directed Surveillance' refers to the use of covert techniques to obtain private information by monitoring a target's movements, conversations and activities other than in residential premises or private vehicles (in simple terms, monitoring a target in public places). This may include: following an SoI; surreptitious photography; tracking a suspect's vehicle; or CCTV. The Director General of MI5 explained that *"what Directed Surveillance generally produces is an understanding of associations, pattern of life, the sort of people these might be; and sometimes behavioural things"*.[158]

170. Directed Surveillance is considered to be less intrusive into an SoI's privacy than Intrusive Surveillance as it takes place in public spaces where there is a lower expectation

---

155 *The Agencies often need to use a combination of intrusive capabilities during an investigation. For example, ***. The law (RIPA and ISA) defines these capabilities separately and sets out different authorisation processes. In such cases, the Agencies may submit an application to the Secretary of State for a combined Property and Intrusive Surveillance Warrant (PSW), which authorises both 'Intrusive Surveillance' under RIPA and 'Interference with Property or Wireless Telegraphy' under ISA. This is specifically allowed for under RIPA Section 42(2) and enables the Minister to consider the necessity and proportionality of the entire operation.*

156 *Written Evidence – SIS, 27 November 2014.*

157 *GCHQ explained that they "sought both Intrusive and Directed Surveillance Authorisations [from the Secretary of State] because we were seeking to *** used by an individual within the UK… Since we were seeking Ministerial authorisation for this, it made sense to include Directed Surveillance in the same submission – if the Secretary of State had rejected the request in respect of the Intrusive Surveillance… it would have been inappropriate for us to authorise Directed Surveillance internally". (Written Evidence – GCHQ, 13 January 2015.)*

158 *Oral Evidence – MI5, 8 May 2014.*

of privacy. In terms of the collateral intrusion (into innocent people's privacy), Directed Surveillance will impact on more people – either through association with the SoI or by being in the same location – but this too is mitigated by the fact that it is conducted in public where people might reasonably expect to be overheard or seen on CCTV, for example.

171. Under RIPA, Directed Surveillance Authorisations (DSAs) are approved internally within the Agencies at 'middle management' grade and are valid for three months.[159] The Intelligence Services Commissioner has statutory responsibility under RIPA for retrospective review of these authorisations. During 2013, a total of *** authorisations were obtained. Of these:

- MI5 authorised the significant majority (***). They explained that most of these related to specific individuals, although in respect of certain investigations *"it is common to maintain a DSA against a specific terrorist group or network… ***"*. They further explained that *"In some longstanding cases, DSAs have been in operation for multiple years… ***"*;[160]
- SIS authorised a far smaller proportion (***). These were used in a number of ways, including *"against individuals to determine their location or pattern of life"* ***;[161] and
- GCHQ authorised a similar proportion (***), some of which covered multiple SoIs.[162]

172. Outside the UK, the Agencies undertake Directed Surveillance on the basis of an authorisation signed by a Secretary of State under Section 7 of ISA. However, there are no figures for the use of this capability outside the UK because it is conducted under a Class Authorisation, and the numbers of operations are not recorded centrally.

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.

b) Interference with Property and Wireless Telegraphy

173. Under the Intelligence Services Act 1994, a Secretary of State may sign a warrant to authorise the Agencies to 'interfere with property or wireless telegraphy':[163]

- ***Property Interference*** involves *"entering, touching, using, damaging or otherwise affecting any property. A common example of this capability is the covert entry and search of an SoI's house or vehicle"*.[164] Property interference also includes IT Operations[165] (i.e. property in the form of electronic devices or

---

159 *The initial DSA is valid for three months, but subsequent extensions may last for up to six months if this is considered to be necessary and proportionate.*

160 *Written Evidence – MI5, 22 August and 27 November 2014.*

161 *Oral Evidence – SIS, 15 May 2014.*

162 *Written Evidence – GCHQ, 20 November 2014.*

163 *ISA warrants remove criminal or civil liability for actions that would otherwise be offences under UK law.*

164 *Written Evidence – MI5, 5 March 2014.*

165 *Also known as Computer Network Exploitation (CNE).*

systems) in order to collect intelligence ***. IT Operations undertaken by the Agencies include operations against:

– a specific device; ***;

– a computer network (***); and

– ***.

- ***Wireless Telegraphy*** involves *"sending or receiving signals over the airwaves rather than using wires. Examples are TV/radio signals, mobile phone signals, GPS/radar/sonar signals and signals sent by remote controls of various kinds"*.[166] Common techniques that the Agencies use to interfere with wireless telegraphy include ***.[167]

The Agencies have explained that these capabilities are usually targeted in relation to specific SoIs or targets. However, we note that, as with other targeted capabilities, there may nevertheless be collateral intrusion into the privacy of innocent people.

EXAMPLE OF INTERFERENCE WITH WIRELESS TELEGRAPHY

***.

***.

***:

***.[168]

Inside the UK

174. Within the UK, action to interfere with property or wireless telegraphy is authorised under a warrant signed by a Secretary of State under Section 5 of ISA. Warrants are valid for six months unless cancelled or renewed (with the Minister's prior agreement). During 2013, the Agencies obtained a total of *** ISA Section 5 Warrants. Of these:

- MI5 obtained the significant majority (***).[169] Around 80% of these related to individual SoIs: these covered covert searches, entry onto property, *** or IT Operations.[170] The remaining 20% of warrants related to multiple SoIs: these covered activities such as *"*** used by multiple SoIs associated with a defined group or network with a common purpose and where the necessity and proportionality considerations are the same"*;[171]

- SIS obtained a far smaller proportion (***). Two-thirds of these warrants related to operations against specific individuals, but the remaining third were

166 *Written Evidence – MI5, 5 March 2014.*

167 *The Agencies' capabilities to interfere with wireless telegraphy under ISA warrants are not the same as their capabilities to intercept the content of communications under the Wireless Telegraphy Act 2006. These capabilities are considered in Chapter 3.*

168 *Oral Evidence – MI5, 8 May 2014.*

169 *Written Evidence – MI5, 22 August 2014. This does not include the combined 'Property and Intrusive Surveillance Warrants' referred to previously.*

170 ****. Written Evidence – MI5, 4 March 2014.*

171 *Written Evidence – MI5, 27 November 2014.*

'thematic' – permitting SIS to use the same technique on multiple occasions. SIS undertook *** 'technical operations' under these warrants ***;[172] and

- GCHQ obtained a similar proportion (***).[173] These primarily authorised IT Operations ***.

175. We note that in certain circumstances the Agencies are able to gain access to an SoI's property under the authority of another organisation's warrant (and therefore do not require an additional specific warrant). The Director General of MI5 explained that:

> *… the authority could be provided, as the first example, by another Agency. So Customs powers, for example. Baggage searches at ports, if Customs have reason to look, then it is done under their authority, not by one of our warrants.*[174]

176. It appears that this process is not overseen by Ministers: in evidence to the Committee, the Home Secretary explained that there was *"no formal process"*[175] by which MI5 would notify her about the use of an authorisation that had been lawfully provided to another department or Agency. In addition, while the Intelligence Services Commissioner has responsibility for reviewing warrants issued under ISA Section 5, he told the Committee that he would not routinely be told about the Agencies' use of another organisation's intrusive powers. In discussion with the Committee, the Commissioner said that he would investigate this issue further.

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.

Outside the UK

177. Outside the UK, operations that involve interference with property are authorised by a Secretary of State under Section 7 of ISA.[176] Both GCHQ and SIS have ISA Section 7 Authorisations enabling them to undertake classes of activities overseas which might otherwise be unlawful under UK law (such as entering onto property or undertaking IT Operations).[177] (ISA Class Authorisations are considered in Chapter 10.) GCHQ operations to interfere with wireless telegraphy are authorised by the Secretary of State under the Wireless Telegraphy Act 2006.[178]

---

172 *Written Evidence – SIS, 3 October 2014.*

173 *Written Evidence – GCHQ, 10 July 2014.*

174 *Oral Evidence – MI5, 8 May 2014.*

175 *Oral Evidence – Home Secretary, 16 October 2014.*

176 *If a target device that is being monitored under the authority of a Section 7 Authorisation is brought into the UK from overseas, the Agencies may continue to interfere with that device for up to five working days under that authorisation. Thereafter, the interference must cease unless it is authorised through a specific ISA Section 5 Warrant. Draft 'Equipment Interference Code of Practice', 6 February 2015.*

177 *GCHQ and SIS have explained that, in addition to the class-based Section 7 Authorisation, they will also seek a specific ISA Section 7 Authorisation from the Secretary of State for operations that use novel or contentious techniques, or else involve significant risks. ISA Section 7 Authorisations are valid for six months (unless extended or cancelled with prior Ministerial agreement).*

178 *The Foreign Secretary has signed a single authorisation covering all of GCHQ's activities under the Wireless Telegraphy Act 2006. There is no time limit to this authorisation, although as a matter of policy the Foreign Secretary is provided with examples of the intelligence derived from this authorisation on an annual basis.*

178. The Committee asked the Agencies how many operations they undertook that interfered with property or wireless telegraphy outside the UK during 2013:

- GCHQ undertook *** operations under Section 7 of ISA authorising them to interfere with computers *** overseas (they may also seek specific authorisation in relation to individual operations).[179]
- SIS explained that they do not hold statistics about the number of operations involving entry onto or interference with property overseas. They told us: *"By their nature, the activities undertaken under the class authorisations on a day-to-day basis encompass the full range of SIS work… data on their use is not held centrally and to record this would be disproportionate"*.[180]
- MI5 officers also undertake operations that involve interference with property or wireless telegraphy overseas: they would seek a warrant from the Home Secretary or Secretary of State for Northern Ireland under Section 5 of the Intelligence Services Act 1994. Where MI5 are acting in support of an SIS operation overseas, this would be authorised through SIS's own ISA Section 7 Authorisation. MI5 were unable to specify the number of operations that they undertook overseas – whether their own or in support of SIS – as their systems are not configured to record this information reliably (for example, details of highly sensitive operations are compartmentalised within MI5).

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.

[179] *These operations vary considerably in both scale and impact. (Written Evidence – GCHQ, 14 November 2014.)*
[180] *Written Evidence – SIS, 27 November 2014.*

IT OPERATIONS: CNE ***

GCHQ conduct IT Operations[181] both within the UK and overseas. During 2013 a significant number (around ***%) of GCHQ's intelligence reports contained information that derived from IT Operations against a target's computer or network[182] – GCHQ call this 'Computer Network Exploitation' (CNE). GCHQ undertook the following CNE operations during 2013:

- ***;[183]
- ***; and
- ***.

In addition to CNE operations to obtain intelligence, ***:

- ***;
- ***; and
- ***.[184]

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.

c) Reading Encrypted Communications

179. Terrorists, criminals and hostile states increasingly use encryption to protect their communications. The ability to decrypt these communications is core to GCHQ's work, and therefore they have designed a programme of work – *** – to enable them to read encrypted communications. There are three main strands to this work:

i) ***;

ii) developing decryption capabilities ***;[185] and

iii) ***.[186]

---

181 *The draft 'Equipment Interference Code of Practice' (6 February 2015) sets out the safeguards that the Agencies must apply in relation to the handling, processing, retention, disclosure and destruction of any information obtained through IT Operations. This includes particular controls for communications that involve legally privileged material, confidential personal information, journalistic material or communications between MPs and their constituents.*

182 *Oral Evidence – GCHQ, 26 June 2014.*

183 *This included *** 'persistent' operations (where the implant 'resides' on an SoI's computer for an extended period) and *** non-persistent operations (where the implant expires when the user's internet session ends).*

184 *Written Evidence – GCHQ, 14 November 2014.*

185 *Commercial encryption products are increasingly provided as standard on common internet services. GCHQ have explained that* ***.

186 ***.

180. The legal basis for this work is the general power afforded to GCHQ under Section 3(1)(a) of the Intelligence Services Act[187] to:

> *… monitor or interfere with electromagnetic, acoustic and other emissions and any equipment producing such emissions and to obtain and provide information derived from or related to such emissions or equipment and from encrypted material.*

No additional Ministerial Authorisation is required for these activities. There are internal procedures: ***.[188] There is no legal requirement to inform Ministers: however, GCHQ have said that they would ask the Foreign Secretary to approve a specific operation of this kind *"where the political or economic risks were sufficiently high"*[189] (although, in practice, they manage their operations to avoid this level of risk). GCHQ told the Committee that:

> *The FCO is aware of the activity and the possible political risk, but individual legal authorisations are not required for each operation. The FCO could assess the political risk of a compromise, it is not well-placed to assess the complex technical risk. Whilst not formally overseen by a Commissioner, the Intelligence Services Commissioner has been briefed on this type of activity where it relates to individual approved operations.*[190]

181. GCHQ's work in this area has been widely criticised. Many people believe, based on the Snowden leaks, that GCHQ systematically undermine and weaken common internet encryption products. For example, Jim Killock of the Open Rights Group said:

> *… techniques used by GCHQ to… take over computers, take control of mobile phones or access networks… rely on things being broken in software that is generally used by companies and individuals very widely…* [This means that GCHQ] *are deciding that their ability to sometimes investigate criminals is more important than the general security of people using software not only in Britain but globally.*[191]

The argument is that this exposes the public to threats from foreign intelligence agencies and cyber criminals, risks undermining trust in digital services generally, and may have a commercial impact on UK communications companies (if customers believe that the companies give the UK Agencies access to their data).

182. We asked GCHQ how they balance the potential intelligence benefits against the inherent security risks ***. GCHQ explained that they have an Information Assurance role, providing government, industry and the public with advice and guidance to protect their IT systems and use the internet safely, ***. Nevertheless, GCHQ said that *"*** our goal is to be able to read or find the communications of intelligence targets"*. The Committee questioned whether this work exposed the public to greater risk. GCHQ said that:

> *… we have increasingly taken into account the interests of members of the public who will use relevant products: ****.[192]

---

187 *We address the use of the general powers under ISA in Chapter 10.*
188 *Written Evidence – GCHQ, 20 August 2014.*
189 *Written Evidence – GCHQ, 20 August 2014.*
190 *Written Evidence – GCHQ, 20 August 2014.*
191 *Oral Evidence – Jim Killock, 15 October 2014.*
192 *Written Evidence – GCHQ, 20 August 2014.*

183. In terms of software vulnerabilities, GCHQ explained that *"the lion's share of vulnerabilities *** are publicly known…* [but] *vendors haven't yet released a fix for them or, if they have, many users are slow to apply the fix"*. In terms of scale, they explained that *"around 10,000 vulnerabilities in common security products were discovered* [globally] *and publicly logged last year"*. GCHQ themselves discovered a number of vulnerabilities (***) which were reported so that vendors could improve their products. Of these ***.[193] The Director of GCHQ further explained:

> ****. So if you like, the risk, the point about large scale damage to the internet, I believe is wrong, it is misplaced.*[194]

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.**

d) Covert Human Intelligence Sources

184. Covert Human Intelligence Sources (CHIS) are individuals who voluntarily provide information to the Agencies for a variety of reasons (they are commonly referred to as agents).[195] The RIPA '*Covert Human Intelligence Sources Code of Practice*' defines a person as a CHIS if:

> *a. he establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraph (b) or (c);*
>
> *b. he covertly uses such a relationship to obtain information or to provide access to any information to any other person; or*
>
> *c. he covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.*[196]

185. Agents provide intelligence about an individual, group or entity that may be of significant value to the protection of UK national security. The Director General of MI5 has emphasised to the Committee the essential work that agents do:

> *… many of these agents put themselves at risk to do the things they do, to help us protect the country. And some of these people are frankly unrecognised heroes, in terms of the way in which they put themselves at risk to acquire the intelligence we would otherwise never get, that leads us to prevent really serious things happening.*[197]

---

193 *Written Evidence – GCHQ, 21 August 2014.*
194 *Oral Evidence – GCHQ, 15 July 2014.*
195 *Agents are not officers of the intelligence Agencies. ***.*
196 *RIPA 'Covert Human Intelligence Sources Code of Practice', 10 December 2014.*
197 *Oral Evidence – MI5, 8 May 2014.*

186. Within the UK, the rules governing the authorisation of the use or conduct of agents are set out in RIPA Part II, with further detail contained in the RIPA '*Covert Human Intelligence Sources Code of Practice*'. The recruitment and use of agents within the UK is authorised internally within the Agencies. Authorisations are valid for 12 months, and an agent may be tasked multiple times under a single authorisation. During 2013, a total of *** agent authorisations were issued. Of these:

- MI5 issued around half (***).[198] This figure does not include agents who are run on their behalf by the police (MI5 have explained that they run about *** of agents directly, with *** run by the police);
- SIS issued the majority of the remainder, *** for agents and a further *** authorisations for their own officers;[199] and
- GCHQ issued a far smaller proportion (***) to allow their analysts to *** in order to obtain information covertly.[200]

187. Outside the UK, the use of agents is authorised under Section 7 of the Intelligence Services Act. SIS have explained that the Foreign Secretary has signed several Class Authorisations covering the use and conduct of their agents – specific operations using agents are then authorised internally.

- SIS explained that they have around *** agents overseas.[201]
- MI5 explained that they also run agents outside the UK: *"***"*.[202]

Privacy concerns

188. During this Inquiry, the Committee considered three specific concerns in relation to the use of agents:

i) level of authorisation – the use and conduct of agents is authorised at a relatively junior level;

ii) unlawful activities – the extent to which agents may be required to take part in illegal or unethical activities in order to maintain their cover or credibility; and

iii) sub-contracting intrusion – the Agencies can use agents to obtain information that they would not be permitted to obtain themselves (unless they obtained Ministerial Authorisation).

189. The Committee explored these concerns with the Agencies. In terms of authorisations for the use and conduct of an agent:

- MI5 told the Committee that they operate different levels of authorisation depending on the activity that the agent was expected to undertake and the risks

---

198 *Written Evidence – MI5, 22 August 2014.*

199 *Oral Evidence – SIS, 15 May 2014. SIS may obtain agent authorisations in order to develop relationships with targets who are visiting the UK, or to develop a relationship with people who are within the UK in order to get access to very difficult targets overseas. ***.*

200 *Written Evidence – GCHQ, 20 November 2014.*

201 *Oral Evidence – SIS, 15 May 2014.*

202 *Written Evidence – MI5, 27 November 2014.*

involved. For example, where an agent is tasked with the specific objective of obtaining or providing access to legally privileged information, MI5 will seek explicit approval from the Home Secretary.

- SIS explained that a number of ISA Section 7 Class Authorisations cover the typical activities that their agents may be required to undertake (***). However, they emphasised that they would seek specific Ministerial Authorisation in cases where it may be necessary for an agent to participate in an activity that would constitute a serious breach of UK law, or was likely to carry *"significant political risk"*.[203]

190. The issue of the participation of agents in unlawful or unethical activity has been specifically considered by the Committee's Investigator and by Sir Desmond De Silva in his report into State collusion in the Patrick Finucane case, where he states:

> *Where, in exceptional circumstances, it proves necessary to ask CHIS to participate in criminal acts in order to fulfil their authorised conduct, agencies giving such tasking will only now carry out such operations, subject to the most stringent processes and safeguards.*[204]

191. In relation to whether agents provide a means of sub-contracting intrusion, we were told that the Agencies each apply robust processes and safeguards when recruiting and running agents, including providing detailed and tailored training to their agents about what they can and cannot do. They also put great emphasis on the skill and professionalism of their staff who specialise in handling agents to understand the motivations and integrity of their agents. The Director General of MI5 explained:

> *So we operate this as a capability or profession in the Service, where we develop levels of skills for people. ***… we also use psychologists in our work; we call them the Behavioural Science Unit. ***.*[205]

192. SIS explained the processes that they follow to ensure that their agents understand the responsibility to act in a manner that is ethically appropriate:

> *… we spend a great deal of time interacting with our agents and describing in very, very precise terms what the limits are on their activity; where they are given the Class Authorisation and where they would not… we constantly have to strike a balance… between allowing our people to be involved, our agents, and them not crossing any immutable red lines.*[206]

193. Nevertheless, the Committee is concerned that, while it may be possible for MI5 to supervise closely the actions that their agents undertake within the UK, this is less straightforward for SIS when dealing with agents overseas ***.[207] In evidence to the Committee, SIS explained:

> ***.[208]

---

[203] *Written Evidence – SIS, 15 May 2014.*
[204] *'The Report of the Patrick Finucane Review', Sir Desmond De Silva, 12 December 2012.*
[205] *Oral Evidence – MI5, 8 May 2014.*
[206] *Oral Evidence – SIS, 15 May 2014.*
[207] *Written Evidence – SIS, 3 October 2014.*
[208] *Oral Evidence – SIS, 15 May 2014.*

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.

9. AUTHORISATIONS AND ACCOUNTABILITY

➢ The current authorisation process for the Agencies' capabilities is as follows:

- Ministers authorise what are considered to be the most intrusive capabilities;
- officials within the Agencies authorise those capabilities which are considered less intrusive;
- the Agencies' activities are subject to a quasi-judicial[209] retrospective audit by two Commissioners; and
- a Tribunal provides for complaints against the Agencies.

Authorisation: Ministers or judges?

194. Those activities considered to be the most intrusive are authorised by a warrant or other authorisation signed by a Secretary of State, authorising activity to be undertaken by the Agencies which would otherwise be illegal. The capabilities currently authorised by a Secretary of State include:[210]

- Interception of Communications;
- Intrusive Surveillance; and
- Interference with Property.

The Home Secretary authorises warrants submitted by MI5 and the Foreign Secretary authorises warrants submitted by GCHQ and SIS.[211]

195. The question as to who should sign warrants for intrusive activities is one that has been raised by a number of witnesses. Those from within Government considered that Ministers are best placed to sign warrants. The Home Secretary said: *"I think it is important that that decision is taken by somebody who is democratically accountable to the public"*.[212] This was echoed by Sir David Omand, who said:

> *I think it is entirely right that a Minister takes the responsibility on herself or himself to sign the warrant and then answers for the consequences if something terrible happens.*[213]

196. However, other witnesses to the Inquiry from outside Government disagreed, arguing that the public has lost trust and confidence in elected politicians to make these

---

209 *While the two Commissioners are former judges, in their roles as Commissioners they are operating outside the official judicial framework. The Commissioners review not only the Agencies' activities but also where applicable the Ministerial authorisation process.*

210 *When they are carried out in the UK.*

211 *The Secretary of State for Northern Ireland authorises warrants relating to terrorism in Northern Ireland. The legislation does not require that specific Secretaries of State authorise warrants submitted by particular Agencies; therefore, when one Secretary of State is unavailable another will be able to support them by considering applications for warrants in their absence.*

212 *Oral Evidence – Home Secretary, 16 October 2014.*

213 *Oral Evidence – Sir David Omand, 23 October 2014.*

decisions. Contributors felt that judges would be better placed to balance individual and collective 'rights' objectively. For example, Liberty said:

> *It is the proper constitutional function of the independent judiciary to act as a check on the use of State power. Judges are best suited to applying necessary legal tests to ensure that surveillance is necessary and proportionate and their involvement will improve public trust and confidence in the system of surveillance.*[214]

197. There are precedents for judicial approval of warrants. In the UK, police applications for search warrants must be signed by judges. Providing evidence to this Committee, Dr Eric Metcalfe (JUSTICE) said:

> *There is something extraordinary about a situation in which a Secretary of State can authorise intrusion into my private communications and my phone calls, but a judge is needed to get a search warrant for a person's house.*[215]

198. In several countries, authority to approve intrusive activities lies with the judiciary. For example, in the United States the Foreign Intelligence Surveillance Court (known as the FISA Court), which is composed of 11 Federal District Court Judges, considers applications by the US intelligence agencies for approval of electronic surveillance, physical searches and other investigative actions for foreign intelligence purposes.

199. Contributors cited the following reasons for the loss of public trust in Ministers as the most appropriate individuals to authorise warrants:

i) the existing warrantry process is itself institutionally biased in favour of security considerations;

ii) Ministers do not have the time to make nuanced decisions about necessity and proportionality; and

iii) Ministers do not have the correct expertise and are liable to be overly swayed by political considerations.

The Committee acknowledges the concerns expressed by contributors to this Inquiry, recognising the value of independent judicial advice and scrutiny. We have therefore explored these issues with witnesses.

200. The process an application has to go through before it reaches the Secretary of State is detailed and rigorous, and takes into account privacy concerns. (For example, an 8(1) warrant application has to consider the possible extent of any interference with the privacy of the individual and why the intelligence sought cannot be obtained by less intrusive means.) A warrant application would not reach the Home Secretary's desk unless it was considered necessary, proportionate and legal. The Home Secretary explained that the application process involved a number of stages, during which successively more senior officials – with advice from lawyers within the Agency and, where necessary, departmental lawyers – would consider whether the application satisfied the legal requirements. Those that they consider did not meet those tests would never be sent to the Home Secretary. The robustness of the application process means that any applications she receives will

---

214 *Written Evidence – Liberty, 7 February 2014.*

215 *Oral Evidence – Dr Eric Metcalfe (JUSTICE), 15 October 2014.*

already have been rigorously tested, and she told the Committee that as a result she did not refuse many warrantry requests.[216] We have been satisfied, from the evidence we have taken, that the legality of the interception receives considerable time, attention and scrutiny.

201. The Home Secretary confirmed that warrantry decisions take up a significant amount of her time and that she spends at least part of her day, every day, assessing warrant applications. She highlighted that an advantage of Ministers signing warrants is that they have the capacity to deal with warrants immediately when necessary. The Agencies have expressed concern that judges might not have the same availability – although we note that this concern could be alleviated by creating a panel of security-cleared judges, similar to the FISA Court in the USA, who could assess warrant applications immediately.

202. While judges will provide an objective assessment of the law, what has become apparent during the course of this Inquiry is that there is a distinct advantage to authorisation by Ministers. Ministers are well informed about the current nature of the threat and are therefore best placed to assess national security considerations. However, what is more significant is that they can apply a further test, on top of the legal tests, by taking into account the wider context of the warrant application. Given the nature of the Agencies' work, there will be circumstances where it would be lawful to use intrusive powers but there may be political or diplomatic risks involved. For example, there could be potential for significant diplomatic 'fall-out' to any alleged activity, as illustrated in 2013 by the deterioration in the USA's relationship with Germany after it was alleged that the National Security Agency (NSA) was intercepting German Chancellor Angela Merkel's phone. This is where the role of a Minister in authorising warrants is crucial: a Minister would wish to take into account whether any benefits that might come from the actions being proposed by the Agencies would be outweighed by reputational damage to the UK if the action proposed became known to the public. SIS explained that, for this reason, they *"will in all cases seek specific authorisation for any proposed activity likely to carry significant political risks, for instance where there could be the potential to cause embarrassment or prejudice the policies of HMG"*,[217] even if such activity is already covered by an existing Class Authorisation.

203. Therefore, while a judge could only assess a warrant application based on compliance with the law (and we note that judges are not immune to criticism when they make controversial decisions),[218] Ministers can apply an additional test which judges cannot. Judges might therefore approve more warrant applications on the basis of pure legal compliance, whereas a Minister may refuse more applications based on these broader considerations.

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

[216] *Oral Evidence – Home Secretary, 15 October 2014.*

[217] *Written Evidence – SIS, 3 October 2014.*

[218] *In the USA, the FISA Court was subject to considerable criticism in the aftermath of the Snowden allegations. More recently, in the UK, the Investigatory Powers Tribunal was criticised for not finding in favour of privacy campaigners. Amnesty described "a disappointing, if unsurprising, verdict from an overseer that was in part assessing itself" (Amnesty International, 5 December 2014).*

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.

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.)

Authorisation: official level

204. Activities which fall below the threshold requiring a warrant are authorised by officials within the appropriate Agency or department. Capabilities which are authorised at official level include:

- activities undertaken by a Covert Human Intelligence Source (CHIS);
- acquisition and disclosure of Communications Data; and
- Directed Surveillance.

205. Officials also authorise individual operations conducted under Section 7 Class Authorisations signed by the relevant Secretary of State under the Intelligence Services Act 1994. ISA does not regulate this internal authorisation process or specify the seniority of the authorising officer. (ISA Class Authorisations are considered in the next chapter.)

ETHICS AND CULTURE

While official authorisations are governed by an internal process, what is important is how staff within the Agencies actually behave. As Sir David Omand highlighted:

> *… self-regulation is the most important form of regulation… You can have all the rules and all the oversight, but when they are out of your sight, you have to rely on the fact that they have internalised a code of values.*[219]

While it will never be possible to safeguard against a 'rogue' employee, the Agencies have highlighted the importance of the robust ethical frameworks governing their activities, and the strong culture and ethos of personal responsibility among their staff. For example, during the Committee's public evidence session in November 2013, the former Director of GCHQ said:

> *My people are motivated by saving the lives of British forces on the battlefield, they are motivated by fighting terrorists or serious criminals, by meeting that foreign intelligence mission as well. If they were asked to snoop, I would not have the workforce. They would leave the building.*[220]

---

[219] *Oral Evidence – Sir David Omand, 23 October 2014.*
[220] *Oral Evidence – GCHQ, 7 November 2013.*

206. The primary argument for some capabilities being authorised at official level is that it reduces the burden on Ministers – if a Minister had to provide authorisation every time an Agency used one of their capabilities, they would have little time for anything else. We therefore recognise that the Agencies cannot seek the approval of Ministers every time they wish to undertake a particular activity, given the impact it would have on the Agencies' work. However, there must be safeguards in place to ensure that official-level authorisations are used appropriately.

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.

Retrospective audit: the Commissioners

207. The Commissioners provide retrospective review of the Agencies: their role is to provide an independent 'audit' of the Agencies' compliance with the law.[221] The Agencies have a statutory responsibility to disclose to the Commissioners all documents or information they require in their oversight role. The Interception of Communications Commissioner is responsible for overseeing the interception of communications and the acquisition of Communications Data by public authorities (including the Agencies). The Intelligence Services Commissioner is responsible for overseeing the use of other intrusive powers by the UK intelligence Agencies.

208. While the Commissioners' roles and some of their work is set out in legislation, the Prime Minister has conferred further responsibilities on them in recent years. For example:

- the Intelligence Services Commissioner provides oversight of the Agencies' holding of Bulk Personal Datasets; and
- ***.

These functions – which cover several important areas of the Agencies' work – are carried out on a non-statutory basis. This should be rectified: the Commissioners themselves have said that they would prefer all of their oversight activities to be placed on a statutory footing.

209. Many of the contributors to this Inquiry argued that the current system of retrospective, quasi-judicial oversight provided by the Commissioners requires reform. Specific points raised by those who gave evidence to us included:

- the Commissioners are not sufficiently independent of the Executive (as they are both appointed by, and report to, the Prime Minister);

[221] *While their role is primarily retrospective, where they have reviewed an application, their views can be taken into account when considering renewal.*

- they are part-time and lack the resources necessary to scrutinise the Agencies properly;
- the secrecy of the Commissioners' work does not inspire public confidence;
- the Commissioners were established in a very different time and context, and therefore their roles now need to be reviewed taking into account changes over the past 25 years (such as technological developments); and
- the sampling regime for reviewing warrants is insufficiently robust given the intrusive nature of these activities.

210. Some contributors specifically recommended that the Commissioners should be replaced by Inspectors General (who exist in several other countries – for example, the USA, South Africa and Australia). However, few provided a substantive explanation of the actual benefits they expected from such a change. In our experience, Inspectors General provide an internal audit function – some even sit within the Agency they oversee. We would therefore question whether such a change would be perceived as improving independence, particularly by comparison with the current system whereby the Commissioners sit outside the Agencies and provide an external audit function.

211. In our view, a more compelling argument is that of time and resources. Where there is scope for increasing capacity, then this should be addressed. For example, it may be possible – at a purely administrative level – to share resources between different parts of the oversight structure, which might offer reduced overheads and economies of scale. (However, we note the need for clear separation between the work of the three bodies – particularly in light of cases brought to the Investigatory Powers Tribunal (IPT) about both the Commissioners and the Intelligence and Security Committee of Parliament.)

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.

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.

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.

Complaints: the Investigatory Powers Tribunal

212. The IPT is a panel of judges and lawyers who hear complaints alleging the unlawful use of covert techniques by public authorities (including the Agencies) which infringe an individual's right to privacy. They also consider claims that the intelligence Agencies have breached other human rights.

213. An example of the matters they consider is the current case in which several non-governmental organisations have alleged that activities undertaken by the Agencies were in contravention of Article 8 (right to privacy) and Article 10 (freedom of expression) of the European Convention on Human Rights. In particular, the IPT has considered the lawfulness of the Agencies' intelligence-sharing arrangements with overseas partners and their 8(4) bulk interception capability.[222]

214. While those who submitted written evidence to this Inquiry felt that the IPT played an important role, many also felt that there are fundamental flaws in how the IPT operates. The concerns they expressed included:

- the practical difficulties of making a case that will be heard in secret;
- the suggestion that the IPT rarely publishes its rulings;
- the IPT has upheld complaints against the Government only in a tiny minority of cases (although we note that as judges they will of course have reached an objective decision depending on the merits of the case before them and therefore we do not consider this a valid argument); and
- there is no right of appeal from the IPT in the UK[223] (in comparison with, for example, the Immigration and Asylum Chamber, which comprises a First-Tier Tribunal and an Upper Tribunal, to allow for cases to be appealed in certain circumstances). Hanne Stevens from Rights Watch UK said: *"Currently, I would say that the individual has no redress or remedy beyond the IPT, which is obviously closed… and this seems to me a very untransparent and unjust way of doing things"*.[224]

215. Witnesses suggested reforms which they considered would increase the transparency of IPT proceedings and decisions and provide for a right of appeal to a higher court. For example, Amnesty International said:

> *It is crucial that complaints against the intelligence services are heard in as transparent a manner as possible in order to ensure the accountability of government agencies with respect to surveillance.*[225]

216. The President of the IPT told the Committee that this is exactly what the Tribunal aims to do. He said that *"there are of course intrinsic difficulties in putting forward and resolving a case in what is inevitably a confidential sensitive area, but that the Tribunal has gone to some considerable lengths to manage and limit those difficulties fairly and as openly as possible"*.[226] He pointed out that *"the Tribunal has overridden some of the precise terms of its rules as being ultra vires,*[227] *and has set out a detailed account of its approach in paragraph 46 of its published judgment of 5 December 2014"*.[228] The President also highlighted that the Tribunal has published numerous judgments (22 of them on its website and/or in official law reports) and has held 10 public hearings

---

222 *IPT/13/77/H, Investigatory Powers Tribunal Judgment, 5 December 2014.*
223 *It is possible to appeal IPT decisions to the European Court of Human Rights in Strasbourg.*
224 *Oral Evidence – Hanne Stevens (Rights Watch UK), 15 October 2014.*
225 *Written Evidence – Amnesty International, 7 February 2014.*
226 *Letter from Sir Michael Burton, President of the Investigatory Powers Tribunal, 12 February 2015.*
227 *In the matter of applications IPT/01/62 and IPT/01/77, dated 23 January 2003.*
228 *IPT/13/77/H, Investigatory Powers Tribunal Judgment, 5 December 2014.*

in the last calendar year, and that in a number of instances important disclosures have been made by the Government as a direct result of intervention by the Tribunal. He noted that:

> *The Tribunal is rare, if not unique, as compared with similar jurisdictions in other countries, in holding public hearings, with advocates for claimants and respondents addressing arguments in open court, upon the basis of assuming a claimant's case to be correct.*[229]

217. While pointing out that in the most recent appeal against a decision of the Tribunal to the European Court of Human Rights in Strasbourg the Court upheld the Tribunal's procedures,[230] the President recognised that a domestic appeal limited to a point of law could be accommodated, although he hoped that it would be a very senior body, such as the Privy Council, which would have a clear understanding of the particular difficulties in this area.

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.

Parliamentary oversight

218. The Intelligence and Security Committee of Parliament (ISC) does not have a formal statutory role itself in authorising or reviewing specific intrusive actions. However, some contributors who provided evidence to this Inquiry suggested reforms to the Committee's composition and working arrangements. These included:

- increased funding and resources, including access to greater professional and technical expertise;[231]
- power to compel witnesses, and the ability to hear evidence from whistle-blowers in confidence;
- an Opposition Chairman;
- a greater role for Parliament in selecting Members;
- removing the Ministerial 'Veto'; and
- responsibility for approving specific intelligence capabilities and intrusive techniques.

219. Parliament considered the structure, procedures and powers of the ISC in July 2013 during the passage of the Justice and Security Act 2013. Major changes were instituted as a result:

- the ISC became a statutory Committee of Parliament;
- the remit was expanded beyond the intelligence Agencies to include the wider intelligence and security activities of the Government;

---

229 *Letter from Sir Michael Burton, President of the Investigatory Powers Tribunal, 12 February 2015.*

230 *Kennedy v United Kingdom [2011] 52 EHRR 4.*

231 *Such expertise can be provided from within the Committee's staff, and it is open to the Committee to request additional expertise where this is felt necessary.*

- the remit was expanded to include operational activity (this is retrospective and on matters of significant national interest, or an Inquiry undertaken at the request of the Prime Minister);
- the ISC can now 'require' information rather than merely 'request' it, as was the case previously;
- Parliament, and not the Prime Minister, now makes the final decision as to who should serve on the Committee;
- the Chairman is chosen by the Committee from its membership, not by the Prime Minister (and can therefore be selected from the Opposition); and
- the Committee's resources, and the manpower available to it, will be greatly increased.

Some of the suggested reforms raised by contributors to this Inquiry were considered by Parliament during passage of the Bill but were rejected.

10. THE LEGISLATIVE FRAMEWORK

➢ In simple terms:

- the Security Service Act 1989 and the Intelligence Services Act 1994 provide the legal basis for the Agencies' activities,
- but that is subject to the overarching requirements of the Human Rights Act 1998,
- and constraints on certain of those activities are set out in other legislation (e.g. RIPA 2000).

220. The legislative framework governing the intelligence and security Agencies in the UK is relatively new. When the Agencies were first publicly avowed, each was placed on a statutory footing – with their functions, authorities and some intrusive powers being set out in the Security Service Act 1989 and the Intelligence Services Act 1994. We have examined the relevant pieces of legislation, and the interaction between them, to assess whether the current statutory framework remains relevant.

a) Interaction between legislation

Security Service Act 1989

221. The Security Service Act 1989 (SSA) sets out the remit of MI5. It gives them statutory authority to obtain or share information in pursuit of their functions (for the protection of national security, the safeguarding of the economic well-being of the UK and the prevention and detection of serious crime). Section 2(2)(a) places a duty on the Director General of MI5 to obtain and disclose information only where necessary in pursuit of their functions (or for the purpose of any criminal proceedings).

Intelligence Services Act 1994

222. The Intelligence Services Act 1994 (ISA) sets out the remit of SIS and GCHQ, giving them statutory authority to obtain or share information in pursuit of their statutory purposes. In broad terms, Section 1 of ISA gives SIS the function to obtain and provide information relating to the actions and intentions of persons outside the British Islands in the interests of the UK's national security or economic well-being, or for the prevention and detection of serious crime. This is then constrained by Section 2(2)(a) which places a duty on the Chief of SIS to ensure that no information is obtained or disclosed by SIS unless it is necessary for the proper discharge of their functions (or for the purpose of a criminal proceeding).

223. Similarly, Section 3(1)(a) of ISA gives the Director of GCHQ the authority to gather information in the interests of the UK's national security or economic well-being, or for the prevention or detection of serious crime. This authority is then constrained by Section 4(2)(a) which places a duty on the Director of GCHQ to ensure that no information is obtained or disclosed by GCHQ unless it is necessary for the proper discharge of their functions (or for the purpose of a criminal proceeding).

THE AGENCIES' PRIORITIES

Both ISA and the SSA use general terms that lack precise legal definition, and this has been criticised by some witnesses to our Inquiry. They suggested that the use of vague terms, such as 'national security', provides wide-ranging powers to the Agencies that are not justified. We questioned the Agencies on this point. MI5 highlighted that the SSA did contain detail as to what their role protecting national security encompassed: *"in particular, its protection from espionage, terrorism and sabotage, from the activities of agents of foreign powers and from actions intended to overthrow or undermine parliamentary democracy"*.[232] GCHQ explained that, in practice (for GCHQ and SIS), 'national security' relates to the priorities set by Ministers through the National Security Council and the Joint Intelligence Committee's annual requirements and priorities process:

> *… our intelligence-gathering priorities are determined by a requirements process, signed off by the National Security Council. This means that GCHQ does not self-task. We work to answer questions set by the Joint Intelligence Committee.*[233]

224. The general powers conferred by ISA and the SSA to obtain and share intelligence are referred to by the Agencies as 'gateways'. The legislation makes clear that these powers can only be undertaken in relation to the Agencies' statutory functions, but contains no further restrictions. The Committee therefore questioned the Chief of SIS on this. He considered that the power under the Intelligence Services Act 1994 was constrained by other legislation:

> *… the Intelligence Services Act is not the only Act that we comply with; it gives us our basic powers, the powers to obtain information and powers to share information through our statutory gateways. And then there are a whole series of legal controls on what we do, around the right to privacy, the Human Rights Act 1998, the Data Protection Act 1998, the RIPA 2000, and so on.*[234]

225. GCHQ also told us that the broad statutory authority under ISA cannot be viewed in isolation. They emphasised that everything GCHQ do must be lawful under the Human Rights Act 1998[235] and that this acts as an overarching constraint: *"GCHQ must ensure that it does nothing that is incompatible with any of the rights set out in the ECHR; the specific Convention right with which GCHQ's activities directly interfere is the right to respect for private and family life"*.[236] All three Agencies confirmed that they must act in accordance with their overarching responsibilities under human rights law. In terms of intrusive activities, Section 6 of the Human Rights Act states that *"It is unlawful for a public authority to act in a way which is incompatible with a Convention right"*.[237]

226. This means that the HRA 'triple test' of legality, necessity and proportionality applies to all of the Agencies' activities. It applies whether or not a specific activity or

---

232 *Security Service Act 1989.*
233 *Oral Evidence – GCHQ, 26 June 2014.*
234 *Oral Evidence – SIS, 15 May 2014.*
235 *The Human Rights Act 1998 gives effect in UK law to protections set out in the European Convention on Human Rights (ECHR).*
236 *Written Evidence – GCHQ, 28 February 2014.*
237 *Human Rights Act 1998, Section 6(1).*

intrusive power is set out in other legislation (such as the Regulation of Investigatory Powers Act 2000), whether or not the activity is carried out under a broad statutory power (such as those provided in ISA and the SSA), and whether or not a power is defined in legislation that pre-dates the UK's Human Rights Act (such as the Telecommunications Act 1984).

227. While the overarching safeguards provided under the Human Rights Act should provide reassurance to the public, the secret nature of the Agencies' work understandably causes some suspicion. This problem is compounded by the fact that the Agencies' powers in the Security Service Act and Intelligence Services Act lack detail and are supplemented by a number of additional intrusive powers set out in other legislation, including:

- the Telecommunications Act 1984;
- the Terrorism Act 2000;
- the Regulation of Investigatory Powers Act 2000;
- the Wireless Telegraphy Act 2006;
- the Counter-Terrorism Act 2008; and
- the Data Retention and Investigatory Powers Act 2014.

228. The interactions between these different pieces of legislation are complicated. GCHQ's solution – in order to be confident that they will always meet their human rights obligations – is to apply the RIPA interception safeguards to all that they do, not just the activities governed by RIPA, since RIPA has been tested and found to be compatible with ECHR requirements.

229. GCHQ have explained to the Committee:

> *Article 8 of the European Convention on Human Rights is the international Gold Standard for the safeguarding of individuals' rights to privacy. This requires that the triple test of legality, necessity and proportionality must be applied whenever a public authority, such as GCHQ, wishes to interfere with those rights… all of our operations that have the potential to infringe upon individuals' privacy are conducted within a legal, policy and cultural framework that at all times fully respects those privacy rights, and fully complies with Article 8. The triple test is embedded in our end-to-end processes at the technological, operational and organisational levels.*[238]

In other words, even where GCHQ are using the implicit authorities contained in ISA, they meet the ECHR requirements of necessity and proportionality by applying the RIPA safeguards which set out in detail how those constraints should operate.

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

[238] *Written Evidence – GCHQ, 28 February 2014.*

activities they deem necessary. We therefore recommend that the Agencies' powers are set out clearly and unambiguously.

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).

b) Class Authorisations

230. In order to fulfil their statutory functions, SIS and GCHQ may be justified in undertaking certain activities abroad that might (without specific authorisations) lead to criminal and civil liability under UK law. For example, SIS may ***. A further example would be GCHQ's operations which might involve infiltrating computers or networks that might fall foul of UK laws relating to computer security and misuse.

231. The Agencies would be unable to fulfil many of their statutory functions without carrying out such activities. Therefore, 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. In signing the authorisation, the legislation specifies that the Secretary of State must be convinced that the proposed action relates to the Agencies' statutory functions, and that it is *"necessary"* and *"reasonable"*. All Section 7 Authorisations last up to six months, after which they must be cancelled or renewed.

SIS

232. SIS have eight class-based Authorisations under Section 7 of the Intelligence Services Act. These remove liability under UK law for day-to-day activity undertaken in pursuit of SIS's statutory functions, such as the identification and use of Covert Human Intelligence Sources, Directed Surveillance and interference with, and receipt of, property and documents.[239]

233. SIS do not have to seek separate authorisation for any individual activities under these eight categories. However, they will seek additional and specific Ministerial Authorisations in certain circumstances:

- where an operation may be particularly contentious, pose specific legal issues or else carries significant political risks (including through the risk of discovery or attribution); or
- where an operation involves the use of a new capability, or where an existing technique is deployed against a new set of targets.

During 2013, SIS obtained *** Section 7 Authorisations related to specific operations.[240]

---

[239] *The full list of SIS's Class Authorisations is as follows:*
i) ***.
ii) ***.
iii) ***.
iv) ***.
v) ***.
vi) ***.
vii) ***.
viii) ***.

[240] *Written Evidence – SIS, 11 November 2014.*

GCHQ

234. As at October 2014, GCHQ had five Section 7 class-based Authorisations. These remove liability under UK law for some activities, including those associated with certain types of intelligence gathering and interference with computers, mobile phones and other electronic equipment.[241]

MI5

235. As set out previously in Chapter 8, MI5 do not use Section 7 Authorisations directly. Where MI5 provide support to operations overseas, their actions are authorised by an ISA Section 7 Authorisation which is sought by SIS. (MI5 are unable to specify how often this has occurred.)

Privacy concerns and safeguards

236. While witnesses to our Inquiry did not raise any concerns regarding authorisations under Section 7, we consider that this is more due to the secrecy surrounding them than a lack of privacy-related concerns. In recent years, many people have expressed suspicion as to the true nature of Section 7 of ISA, with some referring to it as the 'James Bond clause' and suggesting that it might allow serious crimes to be committed.

237. SIS explained to the Committee why they needed Class Authorisations:

> *Class Authorisations cover essential and routine SIS business which might otherwise be unduly delayed by the need to seek a specific authorisation for each occurrence. The requirement to seek individual authorisations for day-to-day business, would also place a significant and disproportionate bureaucratic burden on both SIS operational teams and the Foreign Secretary and FCO officials.*[242]

However, there is a question as to whether *"bureaucratic burden"* is sufficient reason for Class Authorisations. SIS sought to clarify the nature of the impact that a requirement for individual authorisations would have by providing the following example:

> *** [An SIS officer] *may meet a good number of people in the course of a normal working week who are of potential intelligence interest and who are unaware of his or her SIS role. It would be disproportionate both in terms of process and extent of intrusion into privacy to secure separate authorisations to act as a CHIS in each of these cases.*[243]

---

[241] *The full list of GCHQ's Class Authorisations is as follows:*
i) ***.
ii) ***.
iii) ***.
iv) ***.
v) ***.

[242] *Written Evidence – SIS, 3 October 2014.*

[243] *Written Evidence – SIS, 3 October 2014.*

238. In terms of safeguards, Section 7 Authorisations are subject to review and renewal (where necessary) every six months by the Secretary of State. However, Ministers are not kept informed of how Class Authorisations are used.[244] GCHQ and SIS said that they keep the Foreign and Commonwealth Office (FCO) sighted on their activities at official level (in GCHQ's case, through the monthly reporting of all internal approvals) to ensure that the Minister can be briefed on any particular sensitivities, and that *"FCO officials remain aware of activity or have an opportunity to reflect a change in political circumstances"*.[245] However, we note that this is only at official level: there is no further requirement to keep Ministers informed and we therefore question the level of Ministerial awareness.

239. We have also been told that the Intelligence Services Commissioner can review these on a six-monthly basis, checking the necessity and proportionality of activity taking place under Class Authorisations. For example, the Commissioner attends SIS Head Office or stations overseas in order to see how authorisations under Section 7 are being operated on the ground. SIS have explained: *"In carrying out his functions, whether at Head Office or at a station, the Commissioner reviews the material obtained from the authorised acts, interviews the officers responsible for the relevant work and satisfies himself that the statutory requirements have been met"*.[246] Again, it is difficult to see how the reviews can be fully effective if the Agencies do not keep detailed records of the activities they have carried out under such authorisations. The Commissioner told the Committee that he had recommended *"the keeping of a more formal record"*.[247]

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.

---

[244] *GCHQ note that they "provide details about the benefits derived from CNE activities" when applying to the Foreign Secretary to renew the relevant Class Authorisation. (Written Evidence – GCHQ, 7 January 2015.)*

[245] *Written Evidence – GCHQ, 21 August 2014.*

[246] *Written Evidence – SIS, 27 November 2014.*

[247] *Written Evidence – Sir Mark Waller, 4 February 2015.*

c) Exchanging information with overseas partners

Legislative basis

240. The threats to national security that our Agencies are charged with tackling increasingly have an international dimension. Their work therefore includes: running agents in foreign countries, intercepting international communication links and sharing information with other countries where we share a common enemy.

241. As set out previously, under the Intelligence Services Act 1994 and the Security Service Act 1989 the Agencies are authorised to obtain and disclose information in support of their functions.[248] One of the ways in which they use this power is to exchange information with other intelligence agencies. However, the legislation does not contain any detail as to how that exchange should take place or how it should be authorised.

242. Those we have taken evidence from throughout this Inquiry have accepted that, due to the international nature of the threats facing the UK, sharing intelligence with our allies is a fundamental part of the Agencies' work. However, most of our witnesses felt that current intelligence-sharing arrangements are insufficiently regulated, and some suggested that this might provide a mechanism by which the Agencies could circumvent UK legal constraints and human rights protections. Privacy International, for example, argued that *"UK law places no meaningful restrictions on the information that the intelligence and security services can share with and obtain from this* [Five-Eyes] *network"*.[249] Concerns over intelligence-sharing arrangements have increased since revelations regarding the US-run PRISM programme. At the time, the *Guardian* alleged that access to the PRISM programme *"would appear to allow GCHQ to circumvent the formal legal process required to seek personal material such as emails, photos and videos from an internet company based outside the UK"*.[250]

How the Agencies share intelligence

243. The Agencies have long-standing intelligence-sharing agreements with many international partners. Intelligence can be shared raw (i.e. in its original form) or in report form (i.e. it has been analysed and summarised):[251]

- In terms of raw intelligence, GCHQ told the Committee that SIGINT partners can receive intercepted material directly from each other. ***.
- In terms of intelligence reports, GCHQ said that *"our default position is to make all our reported intelligence sharable with our* [Five-Eyes] *partners"*.[252]

---

[248] *Respectively, Section 2(2)(a) (for SIS) and 4(2)(a) (for GCHQ) of the Intelligence Services Act 1994, and Section 2(2)(a) of the Security Service Act 1989 for MI5.*

[249] *Written Evidence – Privacy International, 7 February 2014. The countries comprising the 'Five-Eyes' community are Australia, Canada, New Zealand, the UK and the USA.*

[250] *'UK gathering secret intelligence via covert NSA operation', Guardian, 7 June 2013. As noted previously, the ISC investigated this specific allegation (that GCHQ circumvented UK law) in July 2013. We concluded, in our 'Statement on GCHQ's Alleged Interception of Communications under the US PRISM Programme', that the allegation was unfounded.*

[251] *Some of those who provided evidence to this Inquiry were concerned that the Agencies may have been attempting to circumvent the law by sharing information in report form rather than as raw intelligence. However, the Agencies have a legal basis for both.*

[252] *Written evidence – GCHQ, 28 February 2014.*

Legislation, policy and practice

244. The combination of the Security Service Act, the Intelligence Services Act and the overarching obligations of the Human Rights Act:

- provides the Agencies with legal authority to obtain and share information in pursuit of their functions; but
- forbids the Agencies from obtaining or disclosing any information that is not in pursuit of their functions; and
- requires the Agencies to operate in a manner which does not infringe any ECHR right.

245. The legal framework also requires the Agencies to have appropriate policies in place to govern intelligence sharing (although it lacks any detail as to what those should contain). The Agencies have therefore developed detailed policy arrangements which control the exchange of information with overseas partners. The Director General of the Office for Security and Counter-Terrorism in the Home Office submitted evidence to the Investigatory Powers Tribunal on 16 May 2014, stating: *"The statutory framework* [for sharing information] *is underpinned by detailed internal guidance... and by a culture of compliance"*.[253]

246. The Agencies have explained to the Committee how the legal framework and the policy arrangements apply to intelligence sharing with overseas partners, both in respect of raw, unanalysed intercept material and in respect of analysed and reported intelligence.

i) Exchanging raw intercept

247. The intelligence-sharing arrangements that have attracted the most controversy are those whereby a UK intelligence Agency obtains raw unanalysed material (e.g. raw intercept) from a liaison partner. This has led to allegations that in doing so the Agency is circumventing its obligations under UK law. We have explored this in detail with GCHQ, in particular.

248. GCHQ have explained how these arrangements work in practice using the example of requesting unanalysed interception from the US National Security Agency (NSA).[254]

- In terms of the law:
  - GCHQ are legally allowed to seek intelligence from the NSA in pursuit of their functions under the provisions of the Intelligence Services Act.
  - This includes both intelligence reports (analysed and summarised intelligence) and raw intelligence (original unanalysed intercept).
  - RIPA does not apply in this situation: the safeguards and processes in RIPA, including obtaining interception warrants, can only make lawful actions to which UK law applies.

---

[253] *Charles Farr, Witness Statement to the Investigatory Powers Tribunal, 16 May 2014.*

[254] *While the example relates to sharing material with or receiving material from the US, the same legal and policy constraints would apply in relation to any country.*

- In terms of policy:
  - To ensure that they comply with the Human Rights Act, GCHQ's policy is that where they seek raw intercept from the NSA they follow the procedures and observe the safeguards contained in RIPA (because RIPA has been found to be ECHR compliant). This means that the HRA 'triple test' of legality, necessity and proportionality must be met and a relevant interception warrant needs to be in place – i.e. a Minister has considered that GCHQ are authorised to carry out the interception.[255]
  - GCHQ's request to the NSA would therefore be subject to the same safeguards and scrutiny as those that would be required if GCHQ themselves were carrying out the intrusive activity.
  - GCHQ have adopted this policy as 'belt and braces' – they are applying one set of human rights compliant processes to a slightly different circumstance in order to provide assurance that their dealings with foreign partners are compatible with UK human rights law.
- In terms of practice:
  - GCHQ have never had to seek a warrant solely for the purposes of obtaining raw intercept from an overseas partner. This is because, in practice, GCHQ only ever request intelligence on people if they are already attempting to intercept that person's communications themselves. Their own interception requires an interception warrant authorised by a Secretary of State. Therefore, in practice there has always been an interception warrant in place for any raw intercept GCHQ have sought from their overseas partners.[256]

Therefore, to summarise:

- in legal terms, GCHQ are permitted to seek raw intercept from partners;
- nevertheless, in policy terms, GCHQ would seek *"additional"* Ministerial Authorisation before doing so;
- but, in practical terms, GCHQ have always had Ministerial Authorisation in place before receiving raw intercept from partners because they were already seeking intelligence on the target themselves.[257]

249. While MI5 exchange a broad range of different types of intelligence with overseas partners, raw intercept exchange with overseas partners is not currently a core part of these exchanges. However, MI5 explained that should they receive it they would employ a similar policy and practice. They provided the following example:

---

[255] *Where a RIPA warrant cannot be given because GCHQ cannot conduct the interception themselves, then GCHQ would need to seek the equivalent level of authorisation (i.e. by a Minister). In such circumstances, the safeguards of Section 16 of RIPA also form part of this authorisation.*

[256] *The example we have used refers to one half of the reciprocal arrangement (i.e. GCHQ obtaining intelligence from a foreign partner), but the Committee has been told that the same safeguards also apply to foreign partners obtaining intelligence from GCHQ.*

[257] *The Investigatory Powers Tribunal judgment of 5 December 2014 covered the same ground. We note that the IPT is still to rule on whether the intelligence-sharing provisions of ISA 4(2) etc. are adequate as a matter of law, or whether certain aspects of the policy arrangements that we have set out here need to be codified in legislation.*

> *Were MI5 to ask for* [a Foreign Intelligence Service] *to intercept an individual residing in* [the foreign country] *for the purpose of passing us the raw product, we would consider the situation on a case by case basis. In most instances we would already have a RIPA warrant in place. If a warrant is not already in place, it would be good practice to apply for one (*[unless] *no warrant would be required if the conduct had taken place in the UK). Although this would have no legal validity* [in the foreign country]*, this warrant would serve the same purpose as* [for] *GCHQ… – to demonstrate that we had complied with the requirements of the Human Rights Act 1998 and Article 8 ECHR.*[258]

ii) Exchanging analysed/reported intelligence

250. The Agencies may seek analysed or reported intelligence[259] from their overseas counterparts under ISA (in the case of SIS and GCHQ) or the SSA (in the case of MI5). However, such intelligence sharing is more routine and subject to less stringent arrangements. For example, MI5 described their arrangements for obtaining analysed intelligence from partner agencies overseas as follows:

> *MI5 frequently seeks and obtains a variety of types of intelligence from overseas partners. For example we may write to* [a foreign] *Intelligence Service to seek biographical information on an SOI whom intelligence suggests previously resided in* [the foreign country]. *We do not require a warrant to seek this intelligence (we would not require a warrant to seek this within the UK e.g. from the police). We would seek this intelligence under Section 2(2)a of the Security Service Act. We obtain intelligence of this nature from overseas partners on a regular basis.*[260]

251. We recognise the routine nature of such sharing, and the fact that the Agencies have legal authority to share and seek intelligence. Nevertheless, we questioned whether it should be subject to greater safeguards to give confidence that when intelligence reports are provided to the Agencies, the intelligence has been obtained in a manner compatible with the UK Agencies' obligations under UK law.

252. MI5 explained the processes which they have put in place in order to ensure that they comply with the HRA when receiving and using intelligence reports from a foreign intelligence service. MI5 explained that, in most cases, the intelligence they receive is from liaison partners whom they assess to be human rights compliant. Where they have less confidence in the overseas partner, they will take no action without the approval of senior personnel, in line with the Government's Consolidated Guidance.[261] MI5 also routinely assess incoming intelligence reports to ensure they are relevant to their statutory functions. Where they are not, a record will be kept outlining why no further action will be taken.

253. For their part, GCHQ told the Committee that they would refuse to accept intelligence from a liaison partner if it was obtained through means that would breach UK law. In relation to the NSA (their most significant partner), they said that there is *"a very clear mutual understanding of what is acceptable in legal and policy terms and* [they]

---

[258] *Written Evidence – MI5, 2 March 2015.*

[259] *That is, taking raw intercept, analysing it and placing it in an intelligence report.*

[260] *Written Evidence – MI5, 7 January 2015.*

[261] *'Consolidated Guidance to Intelligence Officers and Service Personnel on the Detention and Interviewing of Detainees Overseas, and on the Passing and Receiving of Intelligence Relating to Detainees', HM Government, July 2010.*

would not offer material that is evidently incompatible with a partner's legal and policy requirements".[262]

254. We also questioned the Agencies on procedures when they receive intelligence material which they have not requested (i.e. it is unsolicited). GCHQ said that when they receive unsolicited intelligence from liaison partners which relates to individuals who live in the UK, they have a Sensitive Receipt Authorisation (SRA) policy to determine whether it is appropriate to accept the material. SRAs are approved internally by a senior official and reviewed at least every six months,[263] although the Director of GCHQ told the Committee in June 2013 that *"The Foreign Secretary has now said that he wishes to receive notice of any SRAs in real time"*. He added that there were at the time *"… two individuals under SRA, *** "*.[264] MI5 explained that they routinely receive unsolicited intelligence from a wide variety of sources. They do not apply separate handling arrangements from those used for solicited material.[265] (We address the receipt of unsolicited material in our proposals for future legislation later in this chapter.)

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.

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.

---

[262] *Written Evidence – GCHQ, 21 August 2014.*

[263] *SRAs that relate to counter-terrorism targets are reviewed every three months. SRAs that relate to non-CT targets are reviewed every six months.*

[264] *Oral Evidence – GCHQ, 27 June 2013.*

[265] *MI5 have explained that their statutory functions do not impose the same restrictions as GCHQ's in terms of individuals in the UK.*

d) Privileged Information

255. A significant privacy concern raised by contributors to this Inquiry is that there are insufficient legal safeguards to protect the communications of certain professions that require privacy in order to carry out their jobs effectively (for instance, lawyers). While RIPA does not specify greater protections for specific professions, the '*Interception of Communications Code of Practice*' does require *"… particular consideration... in cases where the subject of the interception might reasonably assume a high degree of privacy...* [including] *matters subject to legal privilege, confidential personal information or confidential journalistic information"*.[266] However, critics note that a failure to comply with the provisions of a Code of Practice does not render an individual liable to any criminal or civil proceedings.[267] They therefore argue that professional information requires specific protection in legislation.

256. The Committee is sympathetic to this argument. However, we would caveat it with two considerations:

i) an individual who belongs to a specific profession could still pose a threat to national security and therefore the Agencies must still be able to intercept the communications of such individuals (i.e. there should not be a blanket ban); and

ii) there appears to be no agreement as to which professions should be covered. Giving evidence to this Committee, Baroness Onora O'Neill (Equality and Human Rights Commission) said:

> *Special protection requires also special responsibility on the other side. A case can be made for professions in which the communication of data obtained in that way is well regulated, for the medical profession – the one I know best – but also the legal profession. If one is to make the case for journalists, I think it would have to be a completely different case.*[268]

257. We have questioned the Agencies as to the level of protection such material currently receives, taking the example of material subject to Legal Professional Privilege (LPP). Broadly, there are three circumstances where MI5 and GCHQ may intercept LPP material:

i) deliberate interception of lawyer–client communications;

ii) targeted interception of SoIs who happen to be legal professionals; and

iii) incidental interception.[269]

In all three circumstances, the interception must be to meet a national security requirement: the Agencies have emphasised that they would never specifically seek to acquire LPP material.

---

266 *'Interception of Communications Code of Practice', 2007.*

267 *The only route for redress is via a claim in the Investigatory Powers Tribunal.*

268 *Oral Evidence – Baroness Onora O'Neill (Equality and Human Rights Commission), 14 October 2014.*

269 *The Agencies may also acquire legally privileged material as a result of an IT Operation. Within the UK, IT Operations must be authorised by a Secretary of State through an ISA Section 5 Warrant. Outside the UK, such operations would be authorised by a senior official under ISA Section 7 (either a Director for SIS or GCHQ, or the Deputy Director-General in the case of MI5) – draft 'Equipment Interference Code of Practice', 6 February 2015.*

Interception of Privileged Information in the UK

i) Deliberate interception of lawyer–client communications

- MI5 have told the Committee that they do not, as a matter of course, seek to intercept lawyer–client communications. However, in rare circumstances MI5 might apply for a warrant specifically to intercept lawyer–client communications, where it is assessed that it is necessary and proportionate and the intelligence cannot be obtained in a less intrusive way. An example provided by MI5 is:

  … where an imprisoned subject of interest is assessed to be co-ordinating the activities of extremist associates outside the prison by means of communications with the subject's lawyer. If such communications were made with the intention of furthering a criminal purpose, they would in any event not attract legal privilege.[270]

- ***.[271]

ii) Targeted interception of SoIs who happen to be legal professionals

- MI5 may seek to intercept the communications of an SoI who also happens to be a lawyer (i.e. the fact that they are considered a threat to national security is unconnected with their legal work).

iii) Incidental interception

- MI5 may incidentally intercept material which would be covered by LPP through their interception of SoIs. This is the most likely means by which LPP material might be acquired by MI5.

Safeguards

There are a number of handling arrangements and safeguards in place to manage the acquisition of material subject to Legal Professional Privilege:

- Applications to the Home Secretary for 8(1) warrants must specifically assess whether the intercepted material is likely to contain confidential information protected by LPP (and if so, explain why the interception is necessary).
- MI5's internal guidance sets out their procedures for handling this material (for example, using appropriate caveats on the material and limiting disclosure as far as possible).
- Any legally privileged material intercepted and retained by MI5 is made available to the Interception of Communications Commissioner. In cases where there is a high likelihood that LPP material will be obtained as a result of the interception, the Interception of Communications Commissioner is notified of any such warrants.

---

[270] *Written Evidence – MI5, 14 November 2014.*

[271] *MI5 have explained that to provide absolute certainty of this would require a disproportionate amount of research.*

Interception of Privileged Information outside the UK

i) Deliberate interception of lawyer–client communications

- In rare circumstances, GCHQ may specifically target the communications between a lawyer and client if it is considered necessary and justified in order to meet a national security intelligence requirement. ***. (The authorisation process for such interception is set out below.)

ii) Targeted interception of SoIs who happen to be legal professionals

- In some circumstances, GCHQ may target an individual (e.g. a known attack-planner) who also happens to be a lawyer. However, the purpose of the interception is to investigate national security concerns (i.e. targeting them as an SoI) as opposed to investigation of their legal communications. ***.

iii) Incidental interception

- Under bulk interception, it is not technically possible to filter out LPP material, and it may therefore be incidentally collected. However, the fact that it is collected does not mean that it will be examined. It would only become apparent that the material is covered by LPP at the point that it is examined, which GCHQ have said would only happen in *"very exceptional circumstances"*.[272]

- GCHQ may also incidentally intercept material covered by LPP when they target an SoI who is not a lawyer, but who then talks to a lawyer: this will only become apparent if and when the material is examined.

Safeguards

- Given the nature of bulk interception, GCHQ have additional controls and safeguards in place for sensitive material which are triggered at the point at which it is selected for examination.

- If a GCHQ analyst wishes to select for examination the communications of a legal professional located overseas,[273] they are required to obtain an additional internal authorisation ***. This ensures that the specific necessity and proportionality considerations in relation to that material are taken into account. GCHQ have also told the Committee that if an intelligence target is someone who is known to speak regularly to lawyers, an additional internal authorisation may be sought to reflect this (particularly in sensitive cases).

- Such internal authorisations require the approval of the section manager and a centralised team within GCHQ ('GCHQ Mission Policy') and can be granted for a period of up to six months (they can be renewed). These authorisations are reported to the Interception of Communications Commissioner during his inspections.

---

[272] *Written Evidence – GCHQ, 17 November 2014.*

[273] *If the target is located in the UK, GCHQ must seek a 16(3) modification: this is covered in Chapter 5.*

- GCHQ also apply additional controls before issuing any report that includes reference to LPP material and will seek to remove LPP material as much as possible.[274]

Privileged Information within Bulk Personal Datasets

258. SIS may also obtain material attracting LPP through interception, but they have told the Committee that they will only make applications for interception warrants which may involve the interception of legally privileged communications in *"exceptional and compelling circumstances"*.[275] However, SIS are more likely to obtain sensitive information through their acquisition of Bulk Personal Datasets (discussed in Chapter 7). If a bulk dataset contained legally Privileged Information, medical information or journalistic information, it would require *"a higher degree of justification for retention and exploitation"*.[276]

Material relevant to court proceedings in which the Government has an interest

259. All three Agencies also have policies and guidance in place to safeguard against any risk of prejudice or accusation of abuse in circumstances whereby legally privileged material is obtained which is relevant to court proceedings in which they or the Government have an interest. For example, GCHQ told the Committee they implement *"Chinese wall arrangements… to ensure no cross-contamination of… intelligence information to lawyers or policy staff who might be involved in… litigation"*.[277]

260. MI5 have told the Committee that they have guidance in place to ensure that, where interception of a target does result in the acquisition of LPP material, *"MI5 legal advisers do not become aware of the content of legally privileged material that may be relevant to proceedings* [against MI5] *in which they are instructing* [directly] *counsel and in which MI5 has a direct interest in the outcome"*.[278]

261. SIS also have safeguards in place, including *"a detailed policy… governing the potential interception of communications relating to litigation, other legal proceedings or criminal investigations in which SIS or HMG may be a party to or have an interest in"*.[279]

---

[274] *Before being issued, a draft of the Report is given to a centralised team (GCHQ Mission Policy) who, "in consultation with lawyers, will consider whether the material is legally privileged". If a report containing LPP material is issued, it is stamped to make the reader aware of its sensitive content. (Written Evidence – GCHQ, 17 November 2014.)*

[275] *Written Evidence – SIS, 23 December 2014.*

[276] *Written Evidence – SIS, 5 March 2014.*

[277] *Written Evidence – GCHQ, 17 November 2014.*

[278] *Written Evidence – MI5, 14 November 2014.*

[279] *Written Evidence – SIS, 23 December 2014.*

ALLEGATIONS IN THE MEDIA: THE BELHADJ CASE

- On 6 November 2014, several newspapers published allegations that GCHQ had intercepted legally privileged communications between a Libyan politician (Abdul Hakin Belhadj) and his lawyers.
- The articles alleged that information obtained through GCHQ's interception activities may have enabled them to 'rig' ongoing civil and criminal cases that Mr Belhadj had brought against the Government. The allegations were based on internal policy documents that the Agencies had provided in the course of proceedings before the Investigatory Powers Tribunal.
- These were very serious allegations and the Committee sought and received a full explanation of the facts from the Agencies.
- ***.[280]

262. The Government recognises that certain professions require privacy in order to do their jobs effectively and the Agencies have therefore developed internal safeguards to provide greater protection for this information. In February 2015, the Government published for consultation draft Codes of Practice on Interception of Communications and on Equipment Interference. Both documents contained significantly more detail on the protection afforded to such information than has previously been disclosed; this Committee welcomes this move towards greater transparency. However, the Government should use this consultation period as an opportunity to strengthen the safeguards in place for Privileged Information further.[281]

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).

[280] *Written Evidence – GCHQ, 17 November 2014.*

[281] *We note that the Government has already recognised that improvements must be made in a concession to the IPT in February 2015. The Government has accepted that the policies and procedures in place relating to legally privileged material have not been in accordance with human rights legislation. The Committee notes that the Agencies are now working with the Interception of Communications Commissioner to address this.*

e) Telecommunications Act 1984

263. Under Section 94(1) of the Telecommunications Act 1984, the Secretary of State can compel a Communications Service Provider (CSP) to provide assistance to the intelligence Agencies and other government departments under a 'Direction'.[282] The Secretary of State must consider the Direction to be necessary and proportionate in the interests of national security or international relations. While the Direction must be laid before Parliament, this requirement does not apply where the Secretary of State considers such disclosure would be damaging.

264. Several witnesses to our Inquiry have raised concerns that it is unclear what the Telecommunications Act allows the Agencies and other government departments to do and that this lack of transparency needs to be addressed.[283] They argued that all provisions concerning telecommunications should be governed by one piece of legislation, to ensure clarity.

265. The Committee recognises concerns regarding the lack of transparency over the use of these powers. The Agencies explained that providing detailed information publicly about their capabilities derived from Directions under the Telecommunications Act would be significantly damaging to national security – ***.[284]

266. The Committee also has concerns about the safeguards surrounding the use of these Directions: the Telecommunications Act does not contain the detailed safeguards that are inherent in RIPA. The Agencies have assured the Committee that in practice, where the use of the Act interferes with an individual's right to privacy, they apply the principles of legality, necessity and proportionality to justify the assistance they receive through the Telecommunications Act. ***. Further, while the Telecommunications Act does not set a time limit on Directions, as a matter of policy the Agencies review the Directions that interfere with an individual's right to privacy every six months to ascertain whether there is a continuing requirement, and these reviews are subject to oversight by the relevant Secretary of State to ensure that they are satisfied that the Directions remain necessary and proportionate. ***.

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.

---

[282] *The Agencies may also use national security Directions under Section 94 of the Telecommunications Act 1984 for the provision of telecommunications services – these Directions do not impact upon the right to privacy of individuals and we have therefore not included the details in this Report.*

[283] *We refer at paragraph xviii to the question of transparency as a matter of policy and 'foreseeability' as a matter of law.*

[284] ***.

f) Regulation of Investigatory Powers Act 2000

267. The Regulation of Investigatory Powers Act 2000 (RIPA) provides a common legal framework which governs how intrusive capabilities are authorised and controlled. RIPA applies not just to the intelligence and security Agencies, but also to a number of public authorities in the UK. It covers:

- the interception of communications;
- the acquisition and disclosure of Communications Data;
- the carrying out of surveillance (Directed and Intrusive);
- the use of Covert Human Intelligence Sources; and
- methods used to decode encrypted electronic messages.

RIPA is underpinned by Codes of Practice which contain additional detail and guidance (but these are not updated frequently).

Amending RIPA

268. The Agencies' use of these capabilities, and the safeguards constraining that use, have been covered in preceding chapters. Criticism of RIPA has been widespread. The most fundamental objection to the current legislative framework has been that RIPA is out of date: it has been described as 'an analogue law in a digital age' (although this criticism is relevant only to those parts of RIPA dealing with interception of communications and CD).

269. When giving evidence to the Committee, Deputy Chief Constable Jon Boutcher outlined some of the concerns he had as someone responsible for interpreting RIPA:

> *… the legislation isn't fit for the way we now live our lives and the communications challenges that we have. That said, Parliament gave us simple principles to apply, which we always fall back to, around necessity, proportionality and justification… So the principles are sound, but the legislation doesn't fit the challenges we now have in society.*[285]

270. RIPA was designed to be technology-neutral and some witnesses have defended the approach. Sir David Omand, who was the Permanent Secretary at the Home Office during the introduction of RIPA in 2000, explained to the Committee:

> *We could see the internet developing – Hotmail existed, emails existed – so we had some idea. The whole idea was to make it technology-neutral. That is why, for example, we went for a very restricted definition of Communications Data. We did not want to have to keep coming back to Parliament every time somebody developed a new app.*[286]

---

[285] *Oral Evidence – DCC Jon Boutcher, 15 October 2014.*
[286] *Oral Evidence – Sir David Omand, 23 October 2014.*

The Home Secretary told the Committee: *"I think RIPA is still good legislation that is still working well"*.[287]

271. While other witnesses from outside Government expressed a range of views on the merits of the intelligence Agencies having certain intrusive powers, all agreed that the legislative framework was complex, disjointed, vague and lacked transparency. As Professor Charles Raab set out: *"I think RIPA is generally acknowledged to be a bit of a mess"*.[288] We agree that serious reforms are required.

272. However, the complexity of RIPA, together with it being intertwined with a number of other laws governing the Agencies' activities, makes reform difficult. Piecemeal amendments to RIPA and other legislation would only serve to complicate matters further and would not achieve the clarity and transparency we consider necessary.

273. The Committee considers that the time has come for a more radical overhaul of the legislation governing the intelligence and security Agencies. We have set out the principles that the new legislation should cover in the next section.

[287] *Oral Evidence – Home Secretary, 16 October 2014.*
[288] *Oral Evidence – Professor Charles Raab, 15 October 2014.*

g) New legislation to govern the intelligence and security Agencies

274. As we have described throughout our Report, the targeted use of capabilities by the Agencies in general receives broad support. However, there are legitimate concerns around less targeted capabilities. There are also concerns in relation to powers and capabilities that are not clearly defined in legislation.

275. The current legal framework is difficult to understand. It has evolved over time in a piecemeal way through different Acts of Parliament, and the interaction between these pieces of legislation is complicated. It is also unnecessarily secretive. We therefore believe that new legislation is needed. Our recommendations below would consolidate the existing legislation (insofar as it relates to the intelligence and security Agencies only).[289] It would also create a new framework with authorisations and safeguards applied consistently and proportionately and overseen in a more comprehensive way. This would bring much needed clarity and transparency.

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.

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.**

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.

---

[289] *Some legislation, for example RIPA, covers the police and other public bodies. We do not propose that these other bodies should be covered by this new legislation – there should be a clear separation between intelligence and law enforcement functions.*

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.

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.

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.**

11. TRANSPARENCY

276. The Agencies require access to intrusive capabilities, which they must use in secret. The challenge is how to ensure that the public can be confident that these capabilities are being used appropriately.

277. While the UK public appear to – for the most part – be supportive of the Agencies, the National Security Agency (NSA) leaks have led to allegations, myths and misconceptions about the Agencies and these have damaged that trust. Many witnesses to this Inquiry felt that the Agencies need to move 'out of the shadows' in order to retain the confidence of the public over the longer term. The Shadow Home Secretary told the Committee that, in her view, the work of the Agencies:

> *… depends on the framework of consent, and that depends on there being a level of knowledge and understanding as well. I think if we try to keep everything behind closed doors, the danger is that we will undermine the trust that we need for the Agencies to be able to do their work… it is damaging to confidence in the Agencies to try to keep everything too quiet and too silent. You need to build that confidence.*[290]

278. The Government acknowledged the requirement for greater transparency and openness of the Agencies' activities in its written evidence to this Inquiry:

> *The Agencies and the Government... place great value in public confidence, recognising that without the public's support they cannot fulfil their functions, and continually challenge themselves to provide increased transparency of their activities, where this is lawful and not damaging to national security.*[291]

279. However, demands for greater transparency do not sit easily with secret organisations. A delicate balance needs to be struck between the legitimate need for public understanding and consent on the one hand, and the risk of inadvertently damaging operational effectiveness on the other: if the Agencies are completely open about their capabilities then our enemies will learn from that and adapt their behaviours to evade detection. The Director General of MI5 explained:

> *It is necessary, in the end, that the work we do is secret from our adversaries. And so your question goes to the balance of: how far can we go to explain it to the public how we work, without helping the people that we are trying to gain a covert advantage over, which is our adversaries? And that is a difficult one to draw, because even sometimes general things that we say can be of assistance to our adversaries, because they study and analyse and collect this material. And we know of instances where Al Qaeda has made a deliberate study of published material, and particularly material published by Government, in order to learn about how to evade us.*
>
> *And so we are extremely conscious of that. So our first task is to protect the public. That would always be the priority for me. If we can do that, while also explaining*

[290] *Oral Evidence – Rt. Hon. Yvette Cooper, MP, 15 October 2014.*
[291] *Written Evidence – HMG, 7 February 2014.*

what we are doing, I would always want to do that. But I don't want to do anything that compromises the first thing. So that is obviously our approach.[292]

280. It could also be argued that it may be beneficial for adversaries to be 'kept guessing' about the range and scale of the Agencies' capabilities: terrorists' behaviour may be constrained if they believe that the Agencies have more access than they do.

281. The Government has held a firm position in relation to any allegations about the Agencies' capabilities and operations – its long-standing response is that the Government does not comment on intelligence matters. The Government argues that any disclosures relating to the Agencies' capabilities would be the thin end of the wedge, and that the 'Neither Confirm nor Deny' (NCND) policy must be applied consistently in order to work effectively and avoid the risk of inadvertent disclosures that may damage national security.

282. Many contributors to this Inquiry felt that this NCND response was inadequate, given the scale of the NSA leaks and the damage to the Agencies' reputation from misleading reporting. For example, in evidence to the Inquiry the former Home Secretary, the Rt. Hon. David Blunkett, MP, said that such *"old-fashioned paternalism"*[293] was increasingly anachronistic, and that the Government needs to find ways to increase the transparency of intelligence matters in order to maintain public confidence. Professor John Naughton further explained that:

What it comes down to in the end is essentially a proposition "Trust us", and in the past two or three years we have seen a number of startling examples of where serious British public institutions have demonstrated vividly that they are not worthy of trust.[294]

283. Several of the witnesses to the Inquiry identified areas where the Government could be more transparent about the Agencies' work and capabilities. For example, the Equalities and Human Rights Commission submission recommended that *"more could be done to demonstrate to the public that surveillance decisions are made in a manner that respects fundamental rights"*.[295] Sir David Omand commented:

The most important thing is to explain how the system actually works and, as importantly, what it does not allow as well as what it does allow… I think the task is for Ministers, from whatever party, to take the case to the public and, in particular to dispel the illusion that has been created that we are under mass surveillance, because we are not.[296]

284. While there will always be a limit as to what can be said publicly about the Agencies' work, we consider that greater openness regarding the Agencies' activities is essential to improve public understanding of their work and secure confidence and consent. The publication of this Report is an important first step in bringing the Agencies 'out of the shadows'. It has set out in detail the full range of the Agencies' intrusive capabilities, as

---

[292] *Oral Evidence – MI5, 8 May 2014.*
[293] *Oral Evidence – Rt. Hon. David Blunkett, MP, 15 October 2014.*
[294] *Oral Evidence – Professor John Naughton, 15 October 2014.*
[295] *Written Evidence – The Equality and Human Rights Commission, 7 February 2014.*
[296] *Oral Evidence – Sir David Omand, 23 October 2014.*

well as the internal policy arrangements that regulate their use. It has also, for the first time, avowed Bulk Personal Datasets as an Agency capability.

285. However, more must be done. Transparency is a legitimate public expectation,[297] and the Government will need to adopt a more open approach to the Agencies' activities in order to improve understanding and public trust.

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.

[297] *We refer at paragraph xviii to the question of transparency as a matter of policy and 'foreseeability' as a matter of law.*

ANNEX A: FULL LIST OF CONCLUSIONS AND RECOMMENDATIONS

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).

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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).

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.

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.

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).

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.

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.

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.

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.

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.

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.

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.

ANNEX B: THE 2013 ANNUAL REPORT OF THE INTERCEPTION OF COMMUNICATIONS COMMISSIONER

The 2013 Annual Report produced by the Interception of Communications Commissioner, Sir Anthony May, provided a detailed description of the process for obtaining interception warrants under the Regulation of Investigatory Powers Act 2000 (RIPA). Relevant extracts from Sir Anthony's Report are reproduced below. The full Report is available at: http://iocco-uk.info.

Applications for Interception Warrants

3.2 *The main mechanism by which interception of communications may be lawful under RIPA 2000 Part I requires the Secretary of State to issue an interception warrant under Section 5(1). The conduct authorised by an interception warrant includes conduct to obtain the content of the communication and also conduct to obtain related communications data (as defined in Section 20 and Part I Chapter II).*

3.3 *Applicant. An application for an interception warrant cannot be issued except on an application made by or on behalf of the persons listed in Section 6(2) of RIPA 2000. Those persons are;*

- *the Director General of the Security Service (Mi5),*
- *the Chief of the Secret Intelligence Service (Mi6),*
- *the Director of the Government Communications Headquarters (GCHQ),*
- *the Director General of the National Crime Agency,*
- *the Commissioner of the Metropolitan Police,*
- *the Chief Constable of the Police Service of Northern Ireland (PSNI),*
- *the Chief Constable of Police Scotland,*
- *the Commissioners of Customs and Excise (HMRC),*
- *the Chief of Defence Intelligence, Ministry of Defence.*

3.4 *Secretaries of State. Interception warrants have to be authorised personally by a Secretary of State (Section 5(1) and 7(1)(a)). The Secretary of State has to sign the warrant personally, except in an urgent case where the Secretary of State has authorised the issue of a warrant which is then signed by a senior official (Section 7(1)(b)).*

3.5 *There are in practice four Secretaries of State and one Scottish Minister who undertake the main burden of authorising (or declining) interception warrants. The Secretaries of State and Minister mainly concerned are;*

- *the Foreign Secretary;*
- *the Home Secretary;*

- *the Secretary of State for Northern Ireland;*
- *the Defence Secretary; and*
- *the Cabinet Secretary for Justice for Scotland.*[i]

3.6 *Each of the Secretaries of State have senior officials and staff. Their functions include scrutinising warrant applications for their form, content and sufficiency, and presenting them to the relevant Secretary of State with appropriate suggestions.*

3.7 *Statutory necessity purposes. The Secretary of State is forbidden from issuing an interception warrant unless he or she believes that it is* necessary*:*

- *in the interests of national security;*
- *for the purpose of preventing or detecting* serious *crime;*
- *for the purpose of safeguarding the economic wellbeing of the United Kingdom (which has to be directly related to state security).*[ii]
- *for the purpose, in circumstances appearing to the Secretary of State to be equivalent to those in which he would issue a serious crime warrant to give effect to the provisions of any international mutual assistance agreement (Section 5(3)).*

3.8 *These statutory purposes and the requirement of necessity come directly from Article 8 of the Human Rights Convention. To issue an interception warrant for any other purpose would be unlawful. Needless to say, Secretaries of State do not issue interception warrants for other purposes. It is part of my function to make sure that they do not.*

3.9 *Proportionality. The Secretary of State is forbidden from issuing an interception warrant unless he or she believes that the conduct authorised by the warrant is* proportionate *to what is sought to be achieved by that conduct.*

3.10 *Proportionality pervades human rights jurisprudence and is explicitly central to the lawful operation of RIPA 2000. Every application for a Part I Chapter I interception warrant has to address proportionality explicitly. Secretaries of State have to address proportionality in the judgment they apply to decide whether or not to issue an interception warrant. A judgment whether it is proportionate to issue the interception warrant requires holding a balance between (a) the necessity to engage in potentially intrusive conduct and (b) the anticipated amount and degree of intrusion. The judgment has to consider whether the information which is sought could reasonably be obtained by other less intrusive means. This is explicit for interception (Section 5(4)). Warrants are refused (or never applied for) where it is judged that the necessity does not outweigh the intrusion.*

3.11 *Types of Interception Warrants. There are essentially two types of interception warrants. Section 8(1) warrants and Section 8(4) warrants.*

---

[i] *Interception warrants may be issued on "serious crime" grounds by Scottish Ministers, by virtue of arrangements under the Scotland Act 1998. In this report references to the "Secretary of State" should be read as including Scottish Ministers where appropriate. The functions of the Scottish Ministers also cover renewal and cancellation arrangements.*

[ii] *See Directive 97/66/EC.*

3.12 *All interception warrants are for the interception of the content of communications and related communications data.*

3.13 *All interception warrants may comprise communications not identified in the warrant whose interception is necessary in order to do what the warrant expressly authorises (Section 5(6)). These are communications which you cannot technically avoid intercepting if you are going to intercept the communications which the warrant expressly authorises.*

3.14 *All applications for warrants have to be in writing and usually cover several pages. The Secretaries of State have available to them in the applications detailed supporting information including specific sections directed to the protection of privacy.*

3.15 *Interception warrants have an initial duration of* 6 months *where the statutory purpose is national security or economic wellbeing of the United Kingdom, but* 3 months *where the statutory purpose is serious crime (Section 9(6)). They cease to have effect at the end of the period unless they are renewed.*

3.16 *An interception warrant may be renewed at the end of the relevant period by the Secretary of State personally, but only if the Secretary of State believes that it continues to be necessary for a statutory purpose (Section 9(2) and paragraphs 4.13 and 4.14 of the Code of Practice). Applications for renewals have to contain details justifying the necessity for renewal giving an assessment of the intelligence value of the interception to date.*

3.17 *The Secretary of State is required to cancel an interception warrant if he or she is satisfied that it is no longer necessary for the authorised purpose (Section 9(3) and paragraph 4.16 of the Code of Practice). This in practice means that the interception agency should apply for cancellation of a warrant that is no longer necessary.*

3.18 *Exceptionally a warrant may be issued in an urgent case by a senior official if it is expressly authorised by a Secretary of State (Section 7(1)(b), 7(2)(a) and paragraph 4.6 of the Code of Practice). An urgent warrant lasts for 5 days unless it is renewed by the Secretary of State (Section 9(6)(a)).*

3.19 *Section 8(1) interception warrants must name or describe either (a) one person as the interception subject, or (b) a single set of premises as the premises to which the permitted interception relates (Section 8(1) itself). The definition of "person" in Section 81(1) includes any organisation or any association or combination of persons, but that does not detract from the individuality of the required warrant definition.*

3.20 *A Section 8(1) warrant should contain the details required by paragraph 4.2 of the Code of Practice. The required details include:*

- *the background of the operation,*
- *the relevant person or premises the subject of the application;*
- *the communications to be intercepted;*
- *an explanation of the necessity for the interception;*

- *a consideration of why the conduct is proportionate;*
- *consideration of any unusual degree of collateral intrusion, not least if the communications might be privileged; and*
- *an assurance that all intercepted material will be handled in accordance with the safeguards in Section 15 of RIPA 2000.*

3.21 *Section 8(1) warrants have to comprise one or more schedules with details designed to tell the relevant communication service provider (CSP) which communications they are required to intercept (Section 8(2)).*

3.22 *Section 8(4) interception warrants. Section 8(4) disapplies the provisions of Section 8(1) and 8(2) in certain circumstances. This means that a Section 8(4) warrant does not have to name or describe one person as the interception subject or a single set of premises as the target of the interception.*

3.23 *Section 8(4) warrants are restricted to the interception of external communications. External communications are communications sent or received outside of the British Islands (see Section 20).*

3.24 *Section 8(4) warrants should contain the details required by paragraph 5.2 of the Code of Practice. I have for convenience described the statutory structure for Section 8(4) warrants in further detail in Section 6 (Question 5) of this report to which I refer the reader.*

3.25 *Safeguards. These apply to both types of interception warrants. Section 15(2) strictly controls the dissemination of intercepted material. The Section requires that dissemination of intercepted material is limited to the minimum necessary for the authorised purposes. All material (including related communications data) intercepted under Section 8(1) or 8(4) must be handled in accordance with safeguards which the Secretary of State has approved under the duty imposed by RIPA 2000.*

3.26 *Section 15(3) requires that each copy of intercepted material and any related communications data is destroyed as soon as there are no longer grounds for retaining it as necessary for any of the authorised purposes.*

3.27 *There are additional safeguards for Section 8(4) warrants and these are described in Section 6 (Question 5) of this report.*

…

Section 8(1) Interception Warrants

6.5.21 *Procedure for Interception Warrants. This is provided for in Sections 5 to 11 of RIPA 2000 Part I Chapter I and the Code of Practice for the Interception of Communications. The essential features of the application process are included in paragraphs 3.11 to 3.21 of this report.*

6.5.22 *General Safeguards. Section 15 of RIPA 2000 provides for important restrictions on the use of intercepted material. It is an explicit part of my statutory functions under*

Section 57 to keep under review the adequacy of the safeguard arrangements which Section 15 imposes on the Secretary of State. This in the main requires a review of the safeguarding procedures which the interception agencies operate.

6.5.23 *Dissemination. Section 15(2) in substance requires that the dissemination of intercepted material is limited to the minimum that is necessary for authorised purposes. The authorised purposes are those set out in Section 15(4). The main such purpose is that retaining the product of interception continues to be, or is likely to become, necessary for one or more of the original statutory purposes. The restriction on dissemination applies to the number of persons to whom, and the extent to which intercepted material or data is disclosed; the extent to which it is copied and the number of copies made. Copies that are made and retained have to be secure (Section 15(5)). These restrictions have to be considered with Section 19, which (in very short summary) imposes very strict duties of secrecy about matters relating to interception and provides criminal sanctions for breach of those duties.*

6.5.24 *These restrictions on dissemination provide a strong protection against any real intrusion into privacy where for instance lawfully intercepted material, unavoidably obtained, is read or listened to by an analyst and immediately discarded as irrelevant.*

6.5.25 *Destruction. Section 15(3) is important. It provides that each copy made of any intercepted material or related communications data is destroyed no later than when there are no longer grounds for retaining it as necessary for any of the authorised purposes. This has the effect of reducing substantially any risk that the product of interception might be used indiscriminately for anything other than an authorised purpose. The requirement to comply with Section 15(3) is at the heart of our Retention, Storage and Destruction investigation described in paragraphs 3.48 to 3.57 of this report.*

6.5.26 *The Section 8(1) element of RIPA 2000 Part I remains, in my view, fit for purpose in the developing internet age. It works just as properly for internet communications where the identifier to be included in the schedule to the warrant is a known internet identifier as it does for more traditional telephony communication.*

Section 8(4) Interception warrants

6.5.27 *The Section 8(4) statutory system has recently given rise to understandable concern.*

6.5.28 *Statutory structure. It is first necessary to explain the difficult relevant statutory structure. I shall attempt to do this as clearly as I may. For clarity, the forms of expression will in part be mine, not necessarily those in the statute.*

6.5.29 *Section 8(4) disapplies the provisions of Section 8(1) and 8(2) in certain circumstances. This means that a Section 8(4) warrant does not have to name or describe one person as the interception subject or a single set of premises as the target of interception. It does not have to have a schedule setting out specific factors identifying the communications to be intercepted.*

6.5.30 *The circumstances in which a Section 8(4) warrant may be issued are that:*

- *the communications to be intercepted are limited to* external communications *and their related communications data;*
- *external communications are communications sent or received outside the British Islands (Section 20);*
- *the warrant may also comprise communications not identified in the warrant whose interception is necessary in order to do what the warrant expressly authorises (Section 8(5));*
- *in addition to the warrant, the Secretary of State has to give a* certificate *describing certain of the intercepted material and certifying that the Secretary of State considers that the examination of this described material is necessary for one or more of the statutory purposes (Section 8(4)b)), which are;*
  - *in the interests of national security,*
  - *for the purpose of preventing or detecting serious crime,*
  - *for the purpose of safeguarding the economic well-being of the United Kingdom.*

6.5.31 *The intercepted material which may be* examined *in consequence is limited to that described in a certificate issued by the Secretary of State. The examination has to be certified as necessary for a Part I Chapter I statutory purpose. Examination of material for any other purpose would be unlawful.*

6.5.32 *Section 15 safeguards apply. The safeguards in Section 15 which apply to all interception warrants apply equally to Section 8(4) warrants – see paragraphs 6.5.22 to 6.5.25. In particular, Section 15(3) requires that each copy of intercepted material and any related communications data is destroyed as soon as there are no longer grounds for retaining it as necessary for any of the authorised purposes.*

6.5.33 *Extra safeguards for Section 8(4) warrants. There are extra safeguards in Section 16 for Section 8(4) warrants and certificates. Parts of Section 16 are in convoluted language and style. I will summarise the relevant bits as clearly as I may.*

6.5.34 *The Section 8(4) intercepted material may only be examined to the extent that its examination:*

- *has been certified as necessary for a Part I Chapter I statutory purpose, and*
- *does not relate to the content of communications of an individual who is known to be for the time being in the British Islands.*

6.5.35 *Thus a Section 8(4) warrant does not generally permit communications of someone in the British Islands to be selected for examination. This is, however, qualified to a limited extent by Sections 16(3) and 16(5).*

6.5.36 *Section 16(3) permits the examination of material acquired under a Section 8(4) warrant relating to the communications of a person within the British Islands if the*

Secretary of State has certified for "the individual in question" *that its examination is necessary for a statutory purposes in relation to a specific period of not more than 6 months for national security purpose or 3 months for serious crime or economic well-being. Since this certificate has to relate to an individual, it is generally equivalent to a Section 8(1) warrant.*

6.5.37 *Section 16(4) and (5) have the effect that material acquired under a Section 8(4) warrant for a person who is within the British Islands may be examined for a very short period upon the written authorisation of a senior official where the person was believed to be abroad but it has just been discovered that he or she has in fact entered the British Islands. This will enable a Section 8(1) warrant or Section 16(3) certificate for that person to be duly applied for without losing what could be essential intelligence.*

6.5.38 *What this all boils down to is that*

- *a Section 8(4) warrant permits the interception of generally described (but not indiscriminate) external communications.*
- *this may only be lawfully* examined *if it is within a description certified by the Secretary of State as necessary for a statutory purpose.*
- *the selection for examination may not be referable to the communications of an individual who is known to be for the time being in the British Islands unless he or she is the subject of an individual authorisation under Section 16(3) or (5).*[iii]
- *the Section 8(4) structure does not permit random trawling of communications. This would be unlawful. It only permits a search for communications referable to individuals the examination of whose communications are certified as necessary for a statutory purpose.*

[iii] *This analysis of what is now Section 16 of RIPA 2000 was in substance explained in Parliament during a House of Lords debate on the bill which became RIPA 2000. At that stage, what is now Section 16 was clause 15 in the bill. Lord Bassam of Brighton, responding to an opposition amendment (subsequently withdrawn) essentially probing whether clause 8(4) would permit "Orwellian trawling", said at Hansard House of Lords Debates for 12 July 2000 at column 323: "It is still the intention that Clause 8(4) warrants should be aimed at external communications. Clause 8(5) limits such a warrant to authorising the interception of external communications together with whatever other conduct is necessary to achieve that external interception. Whenever such a warrant is signed, the Secretary of State must be convinced that the conduct it will authorise as a whole is proportionate--my favourite word--to the objects to be achieved. His decision to sign will be overseen by the interception of communications commissioner. "The next layer of protection is the certificate. Anything that is not within the terms of the certificate may be intercepted but cannot be read, looked at or listened to by any person. Beyond that are the safeguards set out in subsection (2) of Clause 15. Except in the special circumstances set out in later subsections, or if there is an "overlapping" Clause 8(1) warrant, selection may not use factors which are referable to an individual known to be for the time being in the British Islands."*

ANNEX C: WARRANT APPLICATION TEMPLATES

The intelligence Agencies must apply to a Secretary of State for a warrant to authorise the most intrusive activities: this includes targeted interception, bulk interception, Intrusive Surveillance, Interference with Property or Wireless Telegraphy (or IT Operations), and other activities overseas that are authorised under Section 7 of the Intelligence Services Act 1994. The Home Office explained:

> *Secretaries of State have a statutory responsibility to give careful consideration to applications for warrants from the Security and Intelligence Agencies to undertake the most sensitive forms of surveillance, such as the interception of communications and interference with property.*
>
> *For example, the Home Secretary's agreement must be sought if MI5 wants to conduct covert surveillance on residential premises through a surveillance device. She will receive a detailed warrant application and advice from her officials, and must be satisfied that the national security benefits justify the means, and that the proposed action is necessary and proportionate.*
>
> *Warrant applications provide the intelligence background, the means by which the surveillance or interference will take place, and the degree of intrusion involved. If there is any risk that privileged communications will be intercepted as a result of the proposed activity, this is specifically highlighted, along with details of special handling arrangements and safeguards. The Security and Intelligence Agencies must provide this information and the Secretary of State must personally agree to it before any action can take place.*
>
> *For renewals, the requesting Agency must give details of how the warrant has been used, including the benefits gained, in order to inform the Secretary of State's judgement about necessity and proportionality.*
>
> *This process is closely overseen by the Intelligence Services Commissioner and the Interception of Communications Commissioner who regularly inspect and audit the paperwork, processes and policies relating to warrants sought by the Security and Intelligence Agencies and authorised by warrant issuing departments.*
>
> *The following* [templates] *illustrate the considerations and rigour involved in the warrant authorisation process. These* [templates] *are necessarily much shorter and lack the detail contained in real warrant applications in order to avoid revealing sensitive information about national security threats and the capabilities of the Security and Intelligence Agencies.*[298]

The templates are reproduced below.

[298] *Written Evidence – Home Office, 24 February 2015.*

C1. APPLICATION FOR A RIPA 8(1) WARRANT

This document is an example of the kind of application for interception submitted to the Secretary of State under Section 6 of RIPA. This will be accompanied by a warrant instrument for signature by the Secretary of State.

Investigation: *The investigating agency's code-name for the operation.*

Subject: *The person whose communications would be intercepted.*

Communications addresses to be intercepted: *The specific communications addresses (telephone numbers, email addresses etc.) to be intercepted and the relevant Communications Service Provider (CSP).*

Necessity

Threat:

This section sets out:

- *the aims of the operation, for example to investigate individuals believed to be planning acts of terrorism, or to investigate and arrest members of a gang involved in firearms or drug-related criminality;*
- *who the subject of the application is;*
- *how they are involved in the activity of intelligence interest; and*
- *why this is believed to constitute a threat to national security or involvement in serious criminality.*

Means by which identified:

How the agency knows that the communications address to be intercepted is used by the subject.

Expected product:

What information the agency hopes to gain through interception, for example:

- *information about the commission of crimes (for example, the timing of drug importations or the identities of those involved in child abuse) so that the authorities can prevent the crime, arrest the criminals involved, gather evidence to use in a prosecution or prevent evidence from being concealed or destroyed;*
- *information about support for or direct involvement in terrorism; or*
- *time-critical information which could help save lives or prevent serious harm (for example, the whereabouts of a kidnap victim, or plans for an armed robbery or terrorist attack).*

Proportionality

The potential intrusion into the privacy of the subject or of any other person must be proportionate to what is sought to be achieved by the interception.

The agency will set out the anticipated level of intrusion into the subject's privacy, including the extent to which the communications address is believed to be used for legitimate social or business purposes, and what steps they will take to minimise intrusion.

Collateral intrusion:

The agency will also provide an assessment of any anticipated 'collateral intrusion' into the privacy of other individuals who are not the subject of the warrant. For example, a domestic landline may be used by the subject of the warrant for criminal or extremist purposes, and also by other members of their household who are not of intelligence interest. The agency will detail any steps it will take to manage these risks.

Justification:

Why the intelligence sought by the agency could not reasonably be obtained by other means, such as other less intrusive investigative techniques.

LPP or confidential material:

This section will provide an assessment of the risk, if any, that information might be intercepted that is subject to Legal Professional Privilege (LPP) or otherwise of a confidential nature (for example, journalistic, religious or medical information). It must explain the steps the agency will take to manage any such risk and provide assurances that any such information will be handled appropriately.

C2. A RIPA 8(4) WARRANT APPLICATION AND WARRANT

The following documents consist of:

- a template for a submission to the Foreign Secretary for a new Section 8(4) warrant;
- a template for the 8(4) warrant; and
- a template to confirm that an existing 8(4) Certificate applies to the new warrant.

Foreign Secretary

REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA): APPLICATION FOR NEW WARRANT [Number]

ISSUE

A statement that GCHQ seek a new warrant authorising the interception of communications carried by a named CSP.

PREFERRED OPTION AND TIMING

That the Secretary of State issue the warrant by a specified date, together with an explanation of why that date is appropriate. If the Secretary of State agrees, he should sign both the attached instrument and a statement confirming that a particular Certificate applies to the warrant.

Confirmation that the warrant will expire six months from the date of signature.

BACKGROUND

A description of the communications to be intercepted with an explanation of what intelligence requirements such communications are expected to meet, and thus the specific grounds on which the warrant is being sought, as required by RIPA, i.e. one or more of the following: in the interests of national security; for the purposes of preventing or detecting serious crime; and for the purposes of safeguarding the economic well-being of the United Kingdom.

A description of the operational approach to the interception activities.

RISK ASSESSMENT

An assessment of any technical risks associated with the interception activities.

LEGAL ISSUES

A description of any specific legal matters raised by the proposed interception activities, including any risks in domestic or international law.

Confirmation by an accountable GCHQ officer that the requirements of the relevant parts of RIPA have been met, that interception is necessary in the interests of national security, for the purpose of preventing or detecting serious crime, or for the purpose of safeguarding the economic well-being of the United Kingdom, and that the information sought by the interception could not reasonably be obtained by other means.

Signature of the accountable GCHQ officer

Warrant Number

REGULATION OF INVESTIGATORY POWERS ACT 2000
Part I Chapter I Section 5
Interception warrant under the hand of the Secretary of State

To: The Director, GCHQ

In exercise of the power conferred on me by Section 5 of the Regulation of Investigatory Powers Act 2000 and in accordance with the provisions of Section 8(4) of the Act, I hereby authorise you to secure:

i. [a description of the interception as specified in the submission];

ii. such other conduct as is necessary in order to give effect to i. above.

I believe that this warrant is necessary in the interests of [one or more of the following: national security, for the purpose of preventing or detecting serious crime, or for the purpose of safeguarding the economic well-being of the United Kingdom], and that the conduct authorised by this warrant is proportionate to what is sought to be achieved by that conduct. I have also taken into account whether the information which it is thought necessary to obtain under this warrant could reasonably be obtained by other means.

Unless renewed, this warrant shall cease to have effect at the end of six months from the date of signature.

Date of Signature

One of Her Majesty's Principal Secretaries of State

To: The Director, GCHQ

I hereby confirm that Certificate Number [number], issued on [date] in connection with warrants [warrant numbers], which came into force on [date], is also issued in connection with warrant number [number], as required by Section 8(4)(b) of the Regulation of Investigatory Powers Act 2000.

Date of Signature

One of Her Majesty's Principal Secretaries of State

C3. A RIPA 16(3) MODIFICATION APPLICATION AND WARRANT

The following documents consist of:

– a template for a submission to the Foreign Secretary requesting approval for a RIPA 16(3) modification; and

– a template for the modification instrument.

Foreign Secretary

REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA): APPLICATION TO MODIFY SECTION 8(4) CERTIFICATE IN ACCORDANCE WITH SECTION 16(3)

ISSUE

A statement that GCHQ seek to modify Certificate [number] issued under Section 8(4)(b) in accordance with Section 16(3) to permit the selection of material according to a factor referable to individuals known to be in the UK in the interests of national security.

TIMING

Requested date for issue of the modification [which may be "as soon as possible"].

PREFERRED OPTION

That the Secretary of State issue the modification.

Confirmation of concurrence from FCO and Home Office.

That if the Secretary of State agrees, he should sign and date the instrument [number].

Statement that in accordance with the provisions of Section 16(3) the modification will expire three/six months from the date of signature.

Statement that if a further modification of the Section 8(4) Certificate is required, the Secretary of State will be invited to approve a new modification (subject to the urgency provisions provided in the attached instrument).

BACKGROUND

Outline of basis for modification of the Certificate under Section 16(3).

Statement of matters the Secretary of State must consider in deciding whether to sign the Certificate:

- that material intercepted under the authority of a RIPA Section 8(4) warrant can be selected for examination according to factors referable to individuals as certified by the Secretary of State;
- that the selection referable to the individual in question is necessary for one or more of the purposes stated in RIPA Part I Chapter I subsection 5(3)(a), (b) or (c); viz, in the interests of national security, for the purpose of safeguarding the economic well-being of the UK, or for the purpose of preventing or detecting serious crime;

- that the material relates only to communications sent during a period of not more than three/six months specified in the modification; but
- does not require that the factors referable to the individuals so listed are themselves included in the modification to the Certificate.

Statement of how collateral intrusion will be addressed.

RISK ASSESSMENT

An assessment of any technical risks associated with the interception activities.

LEGAL ISSUES

Confirmation that GCHQ legal advisers have checked the text of the instrument, and confirm that it conforms in all respects with the requirements of the Act.

Confirmation by an accountable GCHQ officer that they have personally checked the attached instrument and certify that it conforms in all respects – text, serial numbers and names of targets – to the details given in this submission.

Confirmation by an accountable GCHQ officer that the requirements of the relevant parts of RIPA have been met, that interception is necessary in the interests of national security, for the purpose of preventing or detecting serious crime, or for the purpose of safeguarding the economic well-being of the United Kingdom, and that the information sought by the interception could not reasonably be obtained by other means.

Signature of the accountable GCHQ officer

ANNEX

Names and details of individuals to be added to the Certificate.

Modification Number

REGULATION OF INVESTIGATORY POWERS ACT 2000

Part I Chapter I Section 5

Modification under Section 10(1)(b) of a certificate issued under Section 8(4)(b) (in accordance with Section 16(3)) in connection with warrant numbers [numbers]

To: The Director, GCHQ

1. In the exercise of the powers conferred on me by Section 10(1)(b) of the Regulation of Investigatory Powers Act 2000 ("the Act") and in order to comply with the requirements of Section 16(3) of the Act I hereby modify the Certificate [number] issued under Section 8(4)(b) of the Act in connection with warrant numbers [numbers] as set out below.

2. I certify that it is necessary in the interests of national security to select material for examination according to factors referable to the individuals, known to be for the time being in the British Islands, named or described below:

[Names of individuals described in the Annex]

3. This modification shall issue on signature and will cease to have effect three/six months from that date in accordance with Section 16(3)(a).

Date of Signature

One of Her Majesty's Principal Secretaries of State

C4. A RIPA SECTION 41 WARRANT FOR INTRUSIVE SURVEILLANCE

This document is an example of the kind of application for an Intrusive Surveillance Warrant submitted to the Secretary of State under Section 41 of the Regulation of Investigatory Powers Act 2000.

Investigation: *MI5 code-name for the operation.*

Subject: *Name of the subject of the warrant.*

The warrant should authorise Intrusive Surveillance of the following description:

This section will set out the nature of the Intrusive Surveillance, for example audio eavesdropping, to be conducted.

The above surveillance should operate in respect of the following property:

This section will detail the property within or on which the Intrusive Surveillance is to be conducted.

Necessity

Threat:

This section sets out: • *the aims of the operation, for example to investigate individuals believed to be planning acts of terrorism;* • *latest developments and the current intelligence picture in the operation;* • *who the subject of the application is;* • *how the subject is involved in the activity of intelligence interest; and* • *why this activity is believed to constitute a threat to national security.*

Relevance of property:

How the property where the Intrusive Surveillance is to be conducted is relevant to the investigation, and how it is linked to the subject. For example, it may be the home address of a terrorist where meetings are being held at which plans for attacks are being discussed.

Expected product:

This section will explain the information that MI5 hope to obtain and how this will support the aims of the operation.

In a counter-terrorism case this will often include gaining intelligence and evidence about individuals involved in raising or transferring funds in support of terrorism, recruiting individuals and arranging their travel to join terrorist groups overseas (for example in Syria), planning or providing material support for attacks in the UK or elsewhere, or radicalising vulnerable individuals.

In counter-espionage cases it may include information about the activities and intentions of individuals working for, or on behalf of, hostile foreign intelligence agencies who pose a threat to UK national security.

Proportionality

Operational plan and risk assessment:

This section will explain how MI5 intend to carry out the actions that would be authorised by the warrant, including the plan, the techniques to be used and the risk of compromise.

Intrusion:

This section will set out the anticipated level of intrusion into the privacy of the subject arising from the actions authorised by the warrant. It must also set out whether there is a risk of collateral intrusion into the privacy of anyone else, for example the subject's family or social contacts, and if so what steps will be taken to minimise this. It must also provide assurances about the handling of any information obtained to ensure that its retention and dissemination are lawful and limited to what is necessary. Any intrusion must be proportionate to the investigative aims of the operation.

Justification:

This section will explain why the intelligence sought could not reasonably be obtained by other less intrusive means.

LPP or confidential material:

This section will provide an assessment of the risk, if any, that the actions might lead to information being obtained that is subject to Legal Professional Privilege (LPP) or otherwise of a confidential nature (for example, journalistic, religious or medical information). It must explain the steps MI5 will take to manage any such risk, and must provide assurances that any such information will be handled appropriately.

C5. AN ISA SECTION 5 PROPERTY WARRANT

This document is an example of the kind of application for a Property Warrant submitted to the Secretary of State under Section 5 of the Intelligence Services Act 1994. This will be accompanied by a warrant instrument for signature by the Secretary of State.

Investigation: *MI5 code-name for the operation.*

Subject: *Name of the subject of the warrant.*

This section will detail the property that is the subject of the warrant. This may include, for example, buildings, vehicles, documents and personal items, or land where the property is situated.

The warrant should authorise the following actions:

This section will set out the actions to be carried out in respect of the property, for example gaining covert access to premises and recording information found there. *It would not be in the public interest to describe in detail the kind of actions that may be undertaken, as this would reveal sensitive operational techniques and capabilities. However, MI5 must clearly set out all actions which would otherwise be unlawful if not authorised by the warrant, so that the Secretary of State is clear what he or she is being asked to authorise.*

Necessity

Threat:

This section sets out: • *the aims of the operation, for example to investigate individuals believed to be planning acts of terrorism;* • *latest developments and the current intelligence picture in the operation;* • *who the subject of the application is;* • *how the subject is involved in the activity of intelligence interest; and* • *why this activity is believed to constitute a threat to national security.*

Relevance of property:

How the property is relevant to the investigation, and how it is linked to the subject. For example, it may be the home address of a terrorist where meetings are being held at which plans for attacks are being discussed.

Expected product:

This section will explain the information that MI5 hope to obtain and how this will support the aims of the operation.

In a counter-terrorism case this will often include gaining intelligence and evidence about individuals involved in raising or transferring funds in support of terrorism, recruiting individuals and arranging their travel to join terrorist groups overseas (for example in Syria), planning or providing material support for attacks in the UK or elsewhere, or radicalising vulnerable individuals.

In counter-espionage cases it may include information about the activities and intentions of individuals working for, or on behalf of, hostile foreign intelligence agencies who pose a threat to UK national security.

Proportionality

Operational plan and risk assessment:

This section will explain how MI5 intend to carry out the actions that would be authorised by the warrant, including the plan, the techniques to be used and the risk of compromise.

Intrusion:

This section will set out the anticipated level of intrusion into the privacy of the subject arising from the actions authorised by the warrant. It must also set out whether there is a risk of collateral intrusion into the privacy of anyone else, for example the subject's family or social contacts, and if so what steps will be taken to minimise this. It must also provide assurances about the handling of any information obtained to ensure that its retention and dissemination are lawful and limited to what is necessary. Any intrusion must be proportionate to the investigative aims of the operation.

Justification:

This section will explain why the intelligence sought could not reasonably be obtained by other less intrusive means.

LPP or confidential material:

This section will provide an assessment of the risk, if any, that the actions might lead to information being obtained that is subject to Legal Professional Privilege (LPP) or otherwise of a confidential nature (for example, journalistic, religious or medical information). It must explain the steps MI5 will take to manage any such risk, and must provide assurances that any such information will be handled appropriately.

C6. A COMBINED PROPERTY AND INTRUSIVE SURVEILLANCE WARRANT UNDER RIPA AND ISA

This document is an example of the kind of application for a Property and Intrusive Surveillance Warrant submitted to the Secretary of State under Section 5 of the Intelligence Services Act 1994 and Section 41 of the Regulation of Investigatory Powers Act 2000 (RIPA) as permitted by Section 42 of RIPA. This will be accompanied by a warrant instrument for signature by the Secretary of State.

Investigation: *MI5 code-name for the operation.*

Subject: *Name of the subject of the warrant.*

The warrant should authorise interference with the following property:

This section will detail the property which is the subject of the warrant. This may include, for example, buildings, vehicles, documents and personal items, or land where the property is situated.

The warrant should authorise the following actions:

This section will set out the actions to be carried out in respect of the property, for example gaining covert access to premises and recording information found there. *It would not be in the public interest to describe in detail the kind of actions that may be undertaken, as this would reveal sensitive operational techniques and capabilities. However, MI5 must clearly set out all actions which would otherwise be unlawful if not authorised by the warrant, so that the Secretary of State is clear what he or she is being asked to authorise.*

The warrant should authorise Intrusive Surveillance of the following description:

This section will set out the nature of the Intrusive Surveillance to be conducted, for example audio eavesdropping.

The above surveillance should operate in respect of the following property:

This section will detail the property within which the Intrusive Surveillance is to be conducted.

Necessity

Threat:

This section sets out:

- *the aims of the operation, for example to investigate individuals believed to be planning acts of terrorism;*
- *latest developments and the current intelligence picture in the operation;*
- *who the subject of the application is;*
- *how the subject is involved in the activity of intelligence interest; and*
- *why this activity is believed to constitute a threat to national security.*

Relevance of property:

How the property is relevant to the investigation, and how it is linked to the subject. For example, it may be the home address of a terrorist where meetings are being held at which plans for attacks are being discussed.

Expected product:

This section will explain the information that MI5 hope to obtain and how this will support the aims of the operation.

In a counter-terrorism case this will often include gaining intelligence and evidence about individuals involved in raising or transferring funds in support of terrorism, recruiting individuals and arranging their travel to join terrorist groups overseas (for example in Syria), planning or providing material support for attacks in the UK or elsewhere, or radicalising vulnerable individuals.

In counter-espionage cases it may include information about the activities and intentions of individuals working for, or on behalf of, hostile foreign intelligence agencies who pose a threat to UK national security.

Proportionality

Operational plan and risk assessment:

This section will explain how MI5 intend to carry out the actions that would be authorised by the warrant, including the plan, the techniques to be used and the risk of compromise.

Intrusion:

This section will set out the anticipated level of intrusion into the privacy of the subject arising from the actions authorised by the warrant. It must also set out whether there is a risk of collateral intrusion into the privacy of anyone else, for example the subject's family or social contacts, and if so what steps will be taken to minimise this. It must also provide assurances about the handling of any information obtained to ensure that its retention and dissemination are lawful and limited to what is necessary. Any intrusion must be proportionate to the investigative aims of the operation.

Justification:

This section will explain why the intelligence sought could not reasonably be obtained by other less intrusive means.

LPP or confidential material:

This section will provide an assessment of the risk, if any, that the actions might lead to information being obtained that is subject to Legal Professional Privilege (LPP) or otherwise of a confidential nature (for example, journalistic, religious or medical information). It must explain the steps MI5 will take to manage any such risk, and must provide assurances that any such information will be handled appropriately.

ANNEX D: LIST OF CONTRIBUTORS TO THE INQUIRY

Written evidence

The Committee announced a call for written evidence to the Inquiry on 11 December 2013. Fifty-six substantive written submissions were received: contributors included the Government, the police and the Agencies, NGOs, privacy advocates, the media, members of the public, Members of Parliament and Members of the House of Lords.

Written submissions to the Inquiry have been published on the ISC website (where the authors agreed to publication), along with the transcripts of the (public) oral evidence sessions. They are available at: http://isc.independent.gov.uk/

Oral evidence

Ministers

HOME OFFICE

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

FOREIGN AND COMMONWEALTH OFFICE

The Rt. Hon. William Hague, MP – Former Secretary of State for the Foreign and Commonwealth Office (to 14 July 2014)

The Rt. Hon. Philip Hammond, MP – Secretary of State for the Foreign and Commonwealth Office (from 15 July 2014)

DEPUTY PRIME MINISTER (IN HIS CAPACITY AS LEADER OF THE LIBERAL DEMOCRATS)

The Rt. Hon. Nick Clegg, MP – Deputy Prime Minister

Officials

COMMISSIONERS

The Rt. Hon. Sir Paul Kennedy – Interim Interception of Communications Commissioner (from 29 July to 31 December 2014)

The Rt. Hon. Sir Anthony May – Interception of Communications Commissioner

The Rt. Hon. Sir Mark Waller – Intelligence Services Commissioner

Joanna Cavan – Head of the Interception of Communications Commissioner's Office

Other officials

SECURITY SERVICE (MI5)

Andrew Parker – Director General

Other officials

GOVERNMENT COMMUNICATIONS HEADQUARTERS (GCHQ)

Sir Iain Lobban KCMG CB – Director (to 2 November 2014)

Robert Hannigan – Director (from 3 November 2014)

Other officials

SECRET INTELLIGENCE SERVICE (SIS)

Sir John Sawers KCMG – Chief (to 31 October 2014)

Alex Younger – Chief (from 1 November 2014)

Other officials

Non-Government witnesses

Assistant Chief Constable Richard Berry (Gloucestershire Police) – National Policing Lead for Communications Data

The Rt. Hon. David Blunkett, MP

Deputy Chief Constable Jon Boutcher (Bedfordshire Police) – Former National Policing Lead for the Regulation of Investigatory Powers Act (RIPA) and for Technical Surveillance Units

Emma Carr – Director, Big Brother Watch

The Rt. Hon. Yvette Cooper, MP – Shadow Home Secretary

Charlie Edwards – Director National Security and Resilience Studies, Royal United Services Institute

Peter Gill – Liverpool University

Professor Anthony Glees – University of Buckingham

Rebecca Hilsenrath – Chief Legal Officer, Equality and Human Rights Commission

Jim Killock – Executive Director, Open Rights Group

Dr Eric Metcalfe – Former Director, JUSTICE

Professor John Naughton – Cambridge University

Baroness Onora O'Neill – Chairwoman, Equality and Human Rights Commission

Sir David Omand – King's College London

Professor Charles Raab – Edinburgh University

Dr Julian Richards – University of Buckingham

Isabella Sankey – Policy Director, Liberty

Professor Tom Simpson – Oxford University

Professor Peter Sommer – De Montfort University

Hanne Stevens – Interim Director, Rights Watch UK