Intelligence and Security Committee

Access to communications data by the intelligence and security Agencies

Chairman:
The Rt. Hon. Sir Malcolm Rifkind, MP

Intelligence and Security Committee

Access to communications data by the intelligence and security Agencies

Chairman:
The Rt. Hon. Sir Malcolm Rifkind, MP

Presented to Parliament
by the Prime Minister
by Command of Her Majesty
February 2013

Cm 8514 £8.75

This publication is available for download at www.official-documents.gov.uk

ISBN: 9780101851428

Printed in the UK by The Stationery Office Limited
on behalf of the Controller of Her Majesty's Stationery Office

ID 2537850 02/13 26675

Printed on paper containing 75% recycled fibre content minimum.

CONTENTS

INTRODUCTION

The Inquiry

1. In June 2012, the Government published its Communications Data draft Bill.[1] The Bill is intended to ensure that the police and other public bodies continue to be able to access communications data.

2. The Government invited a Joint Committee of both Houses of Parliament to subject the Bill to pre-legislative scrutiny. However, whilst the Bill will primarily impact on the police, it also covers the intelligence and security Agencies, and therefore the Home Secretary invited the Intelligence and Security Committee (ISC) to contribute to the pre-legislative scrutiny process. The Committee had already commissioned some work in this area and expected to take a close interest in any forthcoming legislation. We decided to consider the draft Bill as one of our usual independent Inquiries: setting our own terms of reference, determining our own priorities, and following where the evidence takes us.

3. Our focus throughout the Inquiry has been the impact on the intelligence and security Agencies. The Joint Committee is conducting a broader, more wide-ranging investigation and we have not sought to duplicate their work. Our conclusions and recommendations are strictly related to the Agencies and the impact of the draft Bill on them: we do not see it as the role of this Committee to form a judgement on the draft Bill's wider implications.

4. In conducting our Inquiry we have maintained a close dialogue with the Joint Committee and have been given access to the material submitted to it. We are grateful to its Chairman, Lord Blencathra, for assisting us in this regard. We have shared our conclusions with the Joint Committee.

5. In conducting our Inquiry we have taken evidence from the Home Office, the Security Service, the Government Communications Headquarters (GCHQ), major UK-based network Communications Service Providers (CSPs) and BAE Systems Detica.

What is communications data?

6. Communications data (CD) is information about a communication. It applies to telephones (both landline and mobile) and to internet-based communications (including email, instant messaging, web browsing and social media).

7. 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 of the person who pays the line rental.
- Mobile telephones: as above, but also the approximate location from which a call/text is made or received by a handset.
- Internet telephony:[2] 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 Protocol (IP) addresses of the computers used.

[1] *Cm 8359.*
[2] *Also known as Voice over Internet Protocol (VoIP) – the best-known example is Skype.*

- Email: the email addresses of the sender and recipient; the date/time of the message; and the IP addresses of the computers used.
- Instant/social messaging:[3] the online username, login name or account name from which a message is sent or received; the date/time the message is sent; and the IP addresses of the computers used.
- Web browsing: the IP address of the device being used to access the internet; the time/date of logon and logoff;[4] and the record of web domains visited.

Content versus data

Communications data does not include the content of the communication – i.e. what is said in a telephone call; the subject, body and attachment(s) of an email; what is typed in an instant message; and postings on social media sites.

Access to content is governed by Part 1, Chapter 1 of the Regulation of Investigatory Powers Act 2000 (RIPA). Permission to access content is given by a warrant signed by a Secretary of State, when they are convinced that such an intrusion is necessary and proportionate.[5] The Government's proposed legislation would not alter these arrangements.

As technology changes, it is important to ensure that the line can still be drawn between content and data. This is particularly true in relation to web browsing histories. The existing guidance on this (the 2007 RIPA Code of Practice on acquisition and retention of CD, which was approved by Parliament and agreed with the CSPs) indicates in broad terms that the first part of a web address is considered to be CD, with the whole address being content. We have not sought to reach a definitive conclusion as to which elements of internet communications and traffic should be deemed to be data and which parts content. However, the Home Office acknowledged that "*the distinction between data and content, you can argue, is muddied in the Internet world*".[6] The opportunity of this primary legislation should be taken to review and clarify the supporting guidance and, in particular, the status of web browsing histories.

8. CD is held by the relevant CSP or Internet Service Provider (ISP). CSPs can be companies such as BT, Vodafone or Virgin Media, which provide access to internet and telephony services through their network infrastructure, but the same term can also be used of application providers, such as Facebook or Twitter.[7] There are several hundred CSPs and ISPs in the UK providing access services. BT, TalkTalk, Sky, Vodafone, O2, Everything Everywhere, Virgin Media and Three are among the largest.

9. CSPs currently retain large quantities of CD for internal business reasons. For example, they keep records of telephone numbers called to allow itemised billing, they hold names, addresses and bank details in order to bill customers, and they monitor and retain information about traffic passing across their networks to help improve the services they offer.

---

[3] *This can include social media sites such as Facebook and Twitter; online mail services such as Hotmail or Yahoo! Mail; and instant messaging services such as MSN Instant Messenger or Google Chat.*

[4] ***.

[5] *In certain other limited circumstances, access to content is possible without a warrant. These include where one or both parties to the communication have given their consent. An example might be a kidnapping case where the police wish to record a call to identify or trace the kidnapper.*

[6] *Oral Evidence – Home Office, 16 October 2012.*

[7] *Such companies are referred to by the Home Office as Application Communications Service Providers, or ACSPs. We have used 'overseas CSPs' throughout this report for clarity.*

The current rules governing access to communications data

10. CD can be used to establish which people were in the vicinity of a particular crime, to discover more information about a target, as evidence in prosecutions, and to help the authorities develop a picture of criminal networks without the need and expense of placing targets or suspects under surveillance.

11. Some public authorities are therefore currently allowed to access the CD that the CSPs hold under Part 1, Chapter 2 of RIPA. The police and law enforcement, the intelligence and security Agencies, and (where relevant) local authorities and other public bodies can request access to CD if, and only if:

- it is necessary for one of the purposes contained in RIPA (e.g. national security, prevention and detection of crime, public safety);
- the information is necessary for the purposes of the investigation that the authority is pursuing;
- the potential intrusion into an individual's privacy is proportionate to the aims of the operation or investigation; and
- the risk of intrusion into the privacy of individuals unconnected with the investigation has also been considered, and is proportionate to the purposes for which the CD is required.

12. The system of internal authorisation that has to be complied with before a public authority can approach a CSP to request disclosure of CD is thorough and rigorous. ***. It is therefore far from being the instant access to personal data sometimes depicted in films or television series (although it can be near real-time in 'threat to life' situations).

The current use of communications data

13. The primary concern about the use of CD is how intrusive it is. The right of citizens to go about their business without interference from the state is an important principle of our way of life. Article 8 of the European Convention on Human Rights (ECHR) states that "*Everyone has the right to respect for his private and family life, his home and his correspondence*", and that:

> *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.*[8]

[8] *European Convention on Human Rights, pp. 10–11.*

14. The Interception of Communications Commissioner reports annually on the use of RIPA powers. He has recorded that around 500,000 applications for CD under Part 1, Chapter 2 of RIPA are made every year by public authorities.[9] We were told by the Home Office that, of these:

- *** % are from the police and law enforcement;[10]
- *** % are from the Agencies; and
- less than 1% are from other bodies (such as local authorities).

15. However, these figures relate to a request for CD about a device (e.g. a mobile telephone). Sometimes individuals may use several devices, and therefore the headline figure of 500,000 CD applications does not mean that 500,000 individuals have been involved.

16. The Home Office does not have information on the number of people that the 500,000 requests relate to. They explained that "*It's very, very difficult to do that*"[11] because it is not always possible to tell how many devices are being used by one person.[12] Whilst the broader picture is not of direct concern to us in this Inquiry, we nevertheless note that such information would be helpful to Parliament and the public in the wider debate.

17. We questioned the Agencies as to how many individuals their *** requests per annum related to, in order to assess the level of intrusion associated with their use of CD. This was difficult for them to measure with precision, for the reasons mentioned above. However, the Agencies did estimate that if they were to make *** applications in any one year, these might be in connection with around *** targets.[13] Whilst they were only able to give an estimate, as opposed to a precise figure, it is nevertheless helpful to have some sense of the size of the issue. We explore in the next section how the Agencies use the CD they access.

---

[9] *HC 496.*

[10] *The Home Office has provided a 'snapshot' of police use of CD in 2010 which shows the following breakdown: murder investigations 11%; kidnap/extortion/blackmail 3%; sexual offences 12%; drugs trafficking 26%; other serious crime 30%; and other crime 17%. Written Evidence – Home Office, 22 June 2012.*

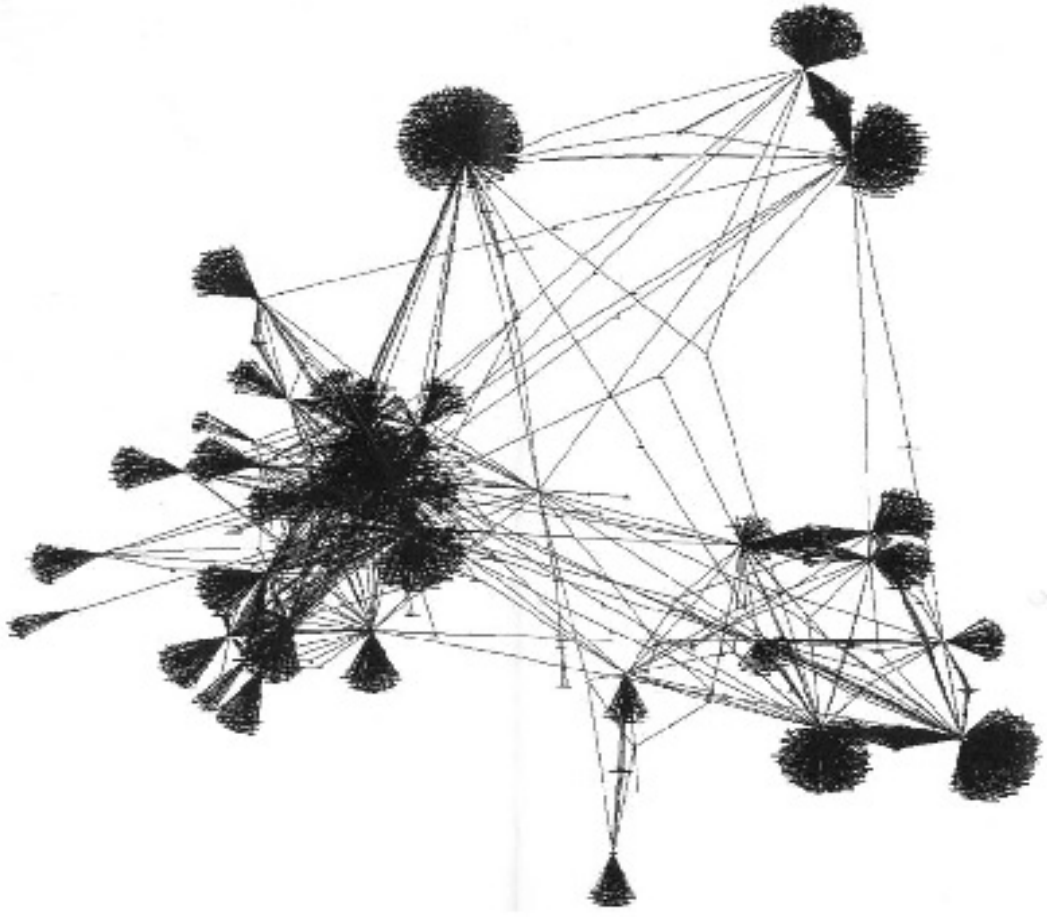
[11] *Oral Evidence – Home Office, 16 October 2012.*

[12] *Work is not always done to match all devices to owners if it is not necessary for the purposes of the investigation. Further, the same request may be made in connection with different investigations (i.e. requests for the same data are duplicated).*

[13] *Some requests may relate to other individuals, who have been in contact with a target but who are then found not to be involved in terrorism or other activities: CD is a very useful tool for ruling subjects of potential interest in or out of investigations at an early stage with minimal intrusion.*

THE AGENCIES' USE OF COMMUNICATIONS DATA

18. The ISC is focused on the need for, and use made of, CD by the intelligence and security Agencies. We are aware from our previous investigations that CD can be immensely valuable: in the ISC's Review of the 7/7 terrorist attacks,[14] the Committee talked of the scale of the 2003–04 Counter-Terrorism (CT) investigation known as Operation CREVICE (an investigation into a group of terrorists who were plotting to detonate a fertiliser bomb in the UK in 2004[15]). At the time, this was the largest operation of its kind ever mounted by the Security Service and during the most intensive part of the investigation more than 4,000 telephone contacts were analysed to try to build a picture of the network of criminals and terrorists associating with the main suspects. The diagram below indicates the scale of the CD involved: each line represents a single communications event (telephone call, text message, etc.) made by those under investigation. The vast majority of these calls or texts were wholly unconnected with attack planning or the wider facilitation network (and may have been as mundane as calling a takeaway restaurant). However, each represented an intelligence lead that the Security Service had to check to see if it was relevant or not.



Communications data seen in connection with Operation CREVICE

19. When we questioned the Agencies during this Inquiry on how they accessed CD, and for what purposes, we were told that the Security Service is by far the greatest user of CD, making *** requests a year under Part 1, Chapter 2 of RIPA (the equivalent figures for GCHQ and the Secret Intelligence Service (SIS) in 2011 are *** and *** respectively). Around half of these

[14] *Cm 7617.*
[15] *In 2007, five men were convicted of offences related to the CREVICE plot.*

applications are for subscriber data only (i.e. the registered owner of a telephone number or email address).[16]

20. The Director General reaffirmed to us the importance of access to CD for the Security Service's investigations. He said:

> *… access to communications data of one sort or another is very important indeed. It's part of the backbone of the way in which we would approach investigations. I think I would be accurate in saying there are no significant investigations that we undertake across the service that don't use communications data because of its ability to tell you the who and the when and the where of your target's activities. It tends to be relatively reliable. It's relatively accessible at the moment in a number of areas, and from our point of view it's a very, very important capability…*
>
> *Obviously what we try to do is to use the tools available to us to identify the activities of people who are putting us at risk and then to act to disrupt that threat…* ***.[17]

21. GCHQ also uses CD – the Director told us: "*Communications data is extremely helpful to us*".[18] However, since most of GCHQ's work is against targets overseas, it makes relatively few requests for CD. Most of these relate to CT or serious crime and, generally, CD is used to help GCHQ determine which targets warrant closer inspection ***. SIS makes less use of CD, with fewer than *** requests a year (***). Given this low usage, we did not take evidence from SIS during this Inquiry.[19]

Intelligence versus evidence

Whilst the Agencies and the police will use CD throughout an investigation, they can use it for quite different purposes.

The Agencies, particularly the Security Service, use CD to develop intelligence leads, to help them focus on those individuals who may be a threat to national security, or to discount individuals seen in contact with those under investigation. The CD they obtain helps to illuminate networks and associations between groups and plots. ***. CD is therefore used *** to help decide quickly, with minimal intrusion and cost, whether contacts of 'subjects of interest' are innocent and of no further interest, or are potential co-conspirators.

Like the Agencies, the police use CD in their investigations. However, the crucial difference is that such data may also represent evidence needed for prosecutions. It is entirely possible that a successful prosecution could hinge on where a mobile phone was at a particular time, when an email was sent between co-conspirators, or the timing of internet messages between gang members. A request for CD may often be made in the final stages of an investigation to corroborate other evidence, possibly about an individual already in custody, charged with an offence, or awaiting trial. (The issue of obtaining CD to evidential standards is primarily a matter for the police and is not therefore one that the ISC has considered.)

[16] *Written Evidence – Home Office, 19 September 2012.*
[17] *Oral Evidence – Security Service, 17 October 2012.*
[18] *Oral Evidence – GCHQ, 18 October 2012.*
[19] *Written Evidence – Home Office, 19 September 2012.*

22. In terms of detailed current or recent operational examples, the Home Office provided this Committee with an overview of the following CT investigations, which demonstrate how CD is typically used in an investigation:

- Tri-Agency CT investigation into terrorist training camps in Pakistan. ***
- Security Service investigation of Al-Qaeda in the Arabian Peninsula attack planning against Western targets. ***
- A Security Service and GCHQ investigation into attack planning in the UK. ***
- A Security Service investigation of a London-based terrorist network involved in UK attack planning. ***

23. In its evidence to the Committee, GCHQ gave further detail on the first of these examples: ***.[20]

- **It is clear to us from the evidence we have been given that communications data is integral to the work of the intelligence and security Agencies and, certainly in terms of the Security Service, it is used in all their investigations.**

- **Whilst communications data can be used throughout an investigation, 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. The easiest, and least intrusive, way of doing so is through access to communications data.**

- **If the Agencies cannot use communications data, then they would need to rely more heavily on other capabilities to provide coverage. However, these other capabilities – such as surveillance or the use of informants – are not like-for-like substitutes, are more intrusive and therefore not always justifiable, and are far more resource-intensive. We therefore consider that it is essential that the Agencies maintain the ability to access communications data.**

[20] *Oral Evidence – GCHQ, 18 October 2012.*

WHAT IS THE CURRENT PROBLEM?

24. The telecommunications industry has seen radical change over the last 20 years, first with the emergence of mobile telephony, and more recently the transition to internet-based communication. The Home Office, police, and the Agencies have explained that this makes the acquisition of CD more difficult. Moreover, the current legislation governing data retention does not cover many of the new forms of communication.

25. Historically, the police and the Agencies could access (when appropriately authorised) the CD they required, which was carried exclusively across the fixed-line telephone network, operated by a single provider, BT. When mobile telephones entered the market, although there were then more service providers, they still retained CD for their internal business reasons (primarily to support the correct billing of customers). This allowed public authorities reasonably complete access to CD under the terms of RIPA.

26. In today's environment, there have been several notable changes:

- As providers have increasingly moved to offering tariffs with unlimited amounts of calls, texts, or data usage, there is no business need for them to retain records of what calls and texts customers make, and details of data used.
- The companies operating fixed line and mobile infrastructure (e.g. BT, Vodafone) are not the same companies providing the services that customers are using (e.g. Facebook, Twitter): in many cases, the network operators simply transport data from another company to the customer with little or no data retained about the communication.
- A complete call or message between two individuals may involve a large number of overseas CSPs and network providers – the data associated with a single communication may therefore be divided among different companies.
- Overseas CSPs, especially those based outside the EU, may not be obliged to retain the CD of most relevance to the authorities. Even if they hold the relevant data, they cannot be obliged to provide it to UK authorities, and may be unwilling to do so voluntarily.

27. As a result of these changes there is now less data being retained by CSPs, and even that which is available is more difficult to access. There has therefore been an erosion of the ability of public authorities to access the CD that they require to support their investigations. The Home Office has referred to this as the 'capability gap'. It estimates that there is a 25% shortfall in the CD that public authorities would wish to access, and what they are currently able to access. It further estimates that, left unchecked, this gap will increase to 35% in two years' time.

28. The calculations behind this figure have been the source of much controversy. The Home Office attempted to explain in its written evidence to the Joint Committee how they arrived at this figure and there has been a great deal of discussion as to how accurate the figure is: the Director General of the Security Service commented in evidence to this Committee that they rested on some "*pretty heroic assumptions*".[21] We have not sought to verify these calculations: whether the gap is 25% or 35% is, in our view, largely immaterial. What is important is whether there is a gap, whether the gap is causing a problem, and – most importantly – how significant that problem is.

29. We questioned the CSPs about the idea of a 'capability gap'. All those we spoke to agreed that it exists and that changing technology and new communications services meant that the gap would continue to grow if left unchecked:

[21] *Oral Evidence – Security Service, 17 October 2012.*

There's certainly a gap undoubtedly, and I think we as [an] industry accept there's a gap… in the coming years that gap will only grow.[22]

30. However, there was concern at the Home Office's attempt to put a precise figure on the size of the problem:

It's actually this 25 per cent gap which is causing the confusion. I don't think the Government have adequately explained that that gap is 25 per cent. I think if it were left as 'there is a gap and we need to close that gap' [it would be easier], but they've actually specifically said 25 per cent, and that's not been properly defined.[23]

- **The fact that there is a problem, if not its precise scale, is easily understood. If the Communications Service Providers are not retaining communications data for internal business reasons, then that data will not be available to the Agencies.**

- **The current gap between the data required by the Agencies and that which the Communications Service Providers – both domestic and overseas – hold for their internal business reasons is significant and, without any action, will continue to grow.**

- **We do not believe that there is any benefit in providing superficially precise estimates of the size of this 'capability gap': unless there is a demonstrable basis for such figures they can be misleading. They can also detract from consideration of the problem itself, which is not necessarily linked to the size of the gap – even a small gap could have a disproportionately large impact.**

[22] *Oral Evidence – Communications Service Providers, 17 October 2012.*
[23] *Ibid.*

WHAT IMPACT WILL THE PROBLEM HAVE ON THE AGENCIES?

31. We have been told that the declining availability of CD is beginning to cause significant problems for public authorities and that the situation will worsen in the coming years. At the current time it is the police and other law enforcement agencies which are most acutely affected. This is a reflection of the lack of viable alternative tools or capabilities available to them, and their use of the data as evidence in prosecutions.

32. The intelligence and security Agencies are less directly affected at the moment because they are able to work around the problem through the use of other national security capabilities.[24] However, the fact that they can cope at the moment should not be taken to mean there is not a problem, as the Director General of the Security Service told us:

> *... the difficulty that we have in* ***.[25]

33. These other national security capabilities only partially overcome the gap in the availability of CD – they are no substitute for a longer-term strategic solution. Some of these capabilities are more costly and more intrusive than might be necessary if there was greater availability of CD. Furthermore, they do not address the fundamental problem of declining CD. In our view, within a few years, it will not be feasible for the Agencies to make up for the decline in CD under the existing legislation by greater reliance on these other capabilities.

34. The Director General of the Security Service stressed the importance of finding a solution for the longer term:

> *In general, it is becoming more difficult to be confident that you are getting CD coverage of the targets that we need to look at, and therefore from our point of view the ability to go some way at least to future-proofing our access to CD is very important.*[26]

- **We have heard numerous examples from the Agencies of communications data playing a vital role in investigations, particularly Security Service Counter-Terrorism operations. If the availability of communications data continues to decline this will have a serious impact.**

- **At present, the intelligence and security Agencies are able, to some extent, to work around the problem of declining communications data by obtaining intelligence using other national security capabilities which are not, in most cases, available to the police. This means that the Agencies are not facing as immediate a problem as that currently faced by the police and other authorities. Nevertheless, we believe that the decline of available communications data will begin shortly to have a serious impact on the intelligence and security Agencies.**

[24] *We have not sought to detail these here.*
[25] *Oral Evidence – Security Service, 17 October 2012.*
[26] *Ibid.*

COMMUNICATIONS DATA – HOW TO TACKLE THE PROBLEM

35. As we have set out, the existing legislation (RIPA) does not cover the problems of emerging technology, or provide the mechanism for asking overseas CSPs to retain CD. Consideration must, therefore, be given to a new approach. There are several options available.

(i) Alternative investigatory tools

36. We have established that CD is central to the Security Service's operations. However, it also has a range of other investigatory tools (e.g. intercepting the content of communications, surveillance, use of informants). We have examined whether greater use could be made of these to offset the decline in the availability of CD. Whilst these other techniques are more intrusive than CD, there are obvious benefits: these investigative tools already exist, are proven to be effective, and do not require further legislation. It would also avoid the CSPs having to retain data that is of no business use to them.

37. However, the Home Office is clear that it has considered, but ruled out, such an approach:

> *We have looked at length, under this Government and the last Government, about whether there are alternatives to [legislation], not least for financial reasons. It's really, really hard to see any. I'm quite sure that there is no non-technical fix. You can't say, 'Okay, we will do more surveillance' or, 'We will do more of some other form of intrusive capability to mitigate this'. It just doesn't work. Nor can we see another technical fix really.*[27]

38. The Director General of the Security Service illustrated the limitations of using alternative tools from the viewpoint of the Agencies:

> *… surveillance, for instance, is an *** expensive *** way of covering somebody's activities. ***.*
>
> *In the same way… we do invest in some operations with undercover officers, but again it's risky and expensive ***; [although] in certain circumstances [it's] the only available option.*[28]

Whilst there are other investigatory tools available, CD is less resource-intensive, quicker and less intrusive than these alternative approaches.

39. We note that some critics of the Communications Data draft Bill have suggested that there may be other investigative options, such as seizing a computer. However, these are post-event, as opposed to acquiring CD, which is used at the beginning of or during an investigation. Furthermore, whilst this may be an option for the police to obtain evidence, it is not an appropriate course of action for the Agencies' covert operations, whether they are pursuing an investigation or a disruption.[29]

---

[27] *Oral Evidence – Home Office, 16 October 2012.*
[28] *Oral Evidence – Security Service, 17 October 2012.*
[29] *The Agencies may not always be in a position to seek prosecutions, and therefore disruptions are sometimes used to mitigate or manage the threat to national security.*

(ii) A voluntary approach

40. During the ISC's evidence sessions, both the Government and representatives from some of the major UK CSPs were very positive about their constructive and collaborative relationship. It did, however, seem to us that there was a qualitative difference in the approach of the CSPs when dealing with CT investigations – we were told that:

> *... when we assess the reputational and other risks involved in working with the Agencies in certain situations, we regard things that are a threat to life and limb through terrorism as frankly much more important...*[30]

41. This raises the question of whether this positive relationship could be used to encourage the CSPs to provide the Agencies with CD on a collaborative, rather than on an enforcement, basis. However, this would require the CSPs to retain data that they do not need for business purposes. In their evidence to us, the CSPs were adamant that this would require a statutory footing. Whilst they recognise that they "*have a responsibility to the country and to the citizens of the country*",[31] the CSPs are clear that they need a legal foundation to retain data.[32] This is particularly true if UK network providers are to be obliged to collect and retain data which is carried on their networks but belongs to another company or service provider – so called 'third-party data' – something that the CSPs told us that they are "*not comfortable [with] at all*".[33] (We address the issue of 'third-party data' at paragraph 58.) Given the stance of the CSPs on the matter, the ISC does not consider that a purely voluntary approach offers a solution.

(iii) The legislative approach

42. The Government has decided that neither expanding the use of alternative investigatory tools nor pursuing a voluntary approach is feasible, and has therefore decided on the legislative route. We accept that, given the drawbacks to the two other options we have examined, this is a logical decision.

43. However, there is a question as to whether existing legislation could be amended, rather than introducing new primary legislation. The Home Office was clear that, although there are many similarities between the relevant part of RIPA and the proposed new legislation, there is a fundamental difference. RIPA is based on the concept of accessing certain pre-existing CD already held by the CSPs for internal business reasons; new legislation would be needed to give the companies the legal basis to collect and retain data they do not need:

> *The legal model at the moment is based on a telephony age. If people collect the data, which companies did, you could ask them to retain it. We have at the moment no power to ask them to collect things they don't need for their business purpose.*[34]

44. We have also considered whether the existing European Data Retention Directive could be used to meet the Government's objective, and avoid the need for new primary legislation. We understand that other countries may be taking this approach. However, we have been told that this would not solve the problem of requiring CSPs to retain data which they have no business need to hold; nor could it apply to non-EU providers. The Directive does not, therefore, address

---

[30] *Oral Evidence – Communication Service Providers, 17 October 2012.*
[31] *Ibid.*
[32] *A legal foundation may also be needed to reimburse CSPs for the costs of storing and providing CD.*
[33] *Oral Evidence – Communication Service Providers, 17 October 2012.*
[34] *Oral Evidence – Home Office, 16 October 2012.*

the ‘capability gap’. Other EU states such as France and Denmark have similarly recognised this problem and have passed their own legislation which goes beyond the Directive.

- **We have examined the possibility of expanding the use of other investigatory tools to offset the decline in availability of communications data, and also whether a voluntary approach might work: neither offers a solution, and indeed the Communications Service Providers themselves have said that they must have a legal foundation to retain data. Whilst legislation is not a perfect solution, we believe it is the best available option.**

THE PROVISIONS OF THE BILL

45. The main provisions of the draft Bill are:

Part 1: Ensuring or facilitating the availability of communications data

- The power for the Secretary of State to make an Order to ensure the availability of CD from CSPs that could be accessed by public authorities, subject to the provisions set out elsewhere in the Bill.
- The power for the Secretary of State to serve individual notices on each CSP that will be required to retain data, specifying the details of what material the particular CSP will have to retain. This would include the ability to instruct CSPs to capture third-party content traversing their networks using technology such as Deep Packet Inspection (DPI).
- CSPs will be able to make representations contesting the contents of a notice to a Technical Advisory Board, which will consider the CSP's argument and make (non-binding) recommendations to the Secretary of State.
- The Bill allows the Secretary of State to take civil proceedings against a company if it fails to comply with a requirement placed upon it.

Part 2: Regulatory regime for obtaining data

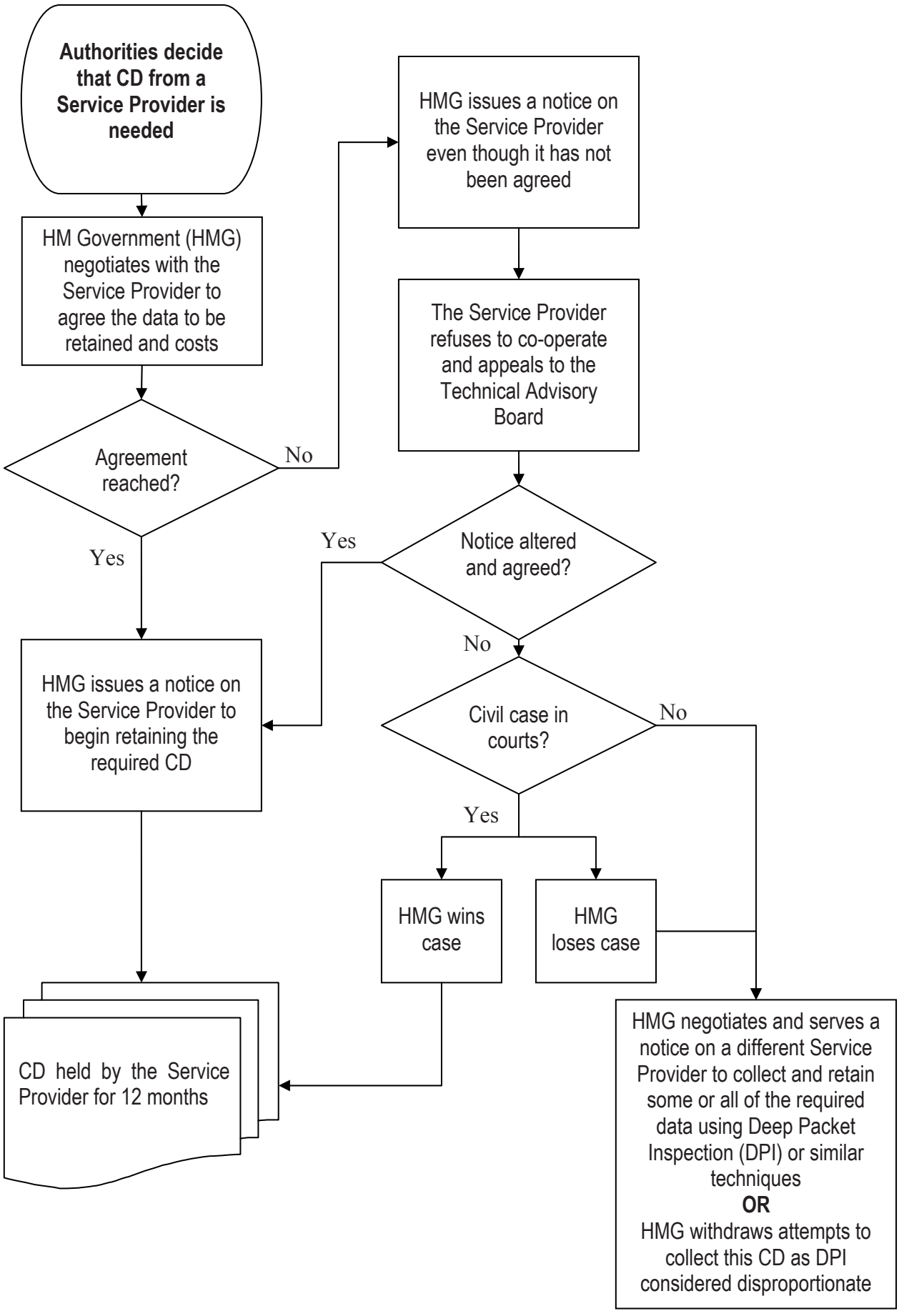
- Part 2 preserves those elements of RIPA which are used to obtain CD from CSPs – in particular, an authorisation to obtain CD may only be granted if the tests of necessity and proportionality are satisfied, and it is necessary to obtain the CD for a permitted purpose (e.g. national security, prevention and detection of crime and disorder).
- Part 2 also allows the Secretary of State to establish a 'filtering' process, which is intended to automate analysis of material requested by public authorities and return the answer to complex queries. In practice this should mean that the volume of CD disclosed to the authority is substantially reduced.

Part 3: Scrutiny and other provisions

- Part 3 reaffirms the existing role of the Interception of Communications Commissioner, and extends it to cover the new filtering arrangements.
- The Information Commissioner will keep under review the security of CD (e.g. against accidental loss, unlawful destruction, unlawful retention, unauthorised disclosure).
- The Investigatory Powers Tribunal will continue its role as a forum for complaints or proceedings relating to conduct by public authorities under RIPA.
- Part 3 also amends certain powers in other legislation so that they may not be used in the future to oblige CSPs to disclose CD.
- Compensating CSPs for the costs of collecting, retaining, disclosing, and otherwise complying with the provisions of the Bill is also covered under Part 3 and is similar to the current framework under RIPA.

46. We understand that the Agencies will be named on the face of the Bill as one of only four bodies having access to the CD powers.

47. The following flow chart illustrates how the elements of the Bill would work in practice:



ARE THESE PROVISIONS WORKABLE?

(i) The Order-making power and notices

48. The draft Bill is very broad in its scope: in particular, it contains a comprehensive power allowing the Secretary of State to make an Order requiring the CSPs to generate and retain CD. We understand that there are two reasons for the broad nature of the Bill:

- to provide flexibility to respond to changes in technology; and
- to mask gaps in investigative coverage.

49. In order to provide sufficient flexibility to future-proof the Bill, the Government has restricted the primary legislation to a broad enabling power: the detail will be contained in notices beneath the legislation. This is because if the detail as to what is and is not covered was on the face of the Bill, then as new technology emerges the primary legislation would need to be amended. The question of whether this is necessary and/or desirable is primarily an issue for the Joint Committee to consider.

50. We have been told that the legislation is also deliberately vague in order to hide the gaps in the authorities' investigative coverage. On one level, this is understandable: for example, if the Bill says that a particular set of data (e.g. relating to text messages) will be covered, then this would reveal (a) that there is currently a problem accessing text message data, and (b) that other forms of CD (e.g. relating to email messages) are not going to be covered. This would give a clear indication to criminals and terrorists as to which forms of communications they should or should not use to escape detection.

51. However, the complete absence of any detail about the data to be covered by the Bill is giving rise to considerable concern in Parliament and from the general public. We have been given detailed evidence as to which areas will and will not be covered and, moreover, which particular types of communications are currently causing the greatest problems. This is highly classified material and could not be made public without damaging the operational capabilities of the Agencies. However, we note that the Joint Committee has been given a very broad indication of the categories of CD that comprise the current gap and which will therefore be covered by the Bill. This is in the form of three broad sets of data: IP address subscriber details; data identifying which internet services or websites are being accessed; and data from overseas CSPs. This information was originally classified as 'Restricted' by the Home Office (the official definition of which includes information which, if made public, may be prejudicial to the investigation of crime, or risk reducing operational effectiveness or security). We questioned whether the generic nature of these categories of data would really cause such damage. There is a balance to be struck between that potential damage, and the damage which would be caused by the failure to generate sufficient confidence in the Bill which might then jeopardise its passage through Parliament. We therefore welcome the fact that the Home Office has now placed this information in the public domain.

52. It is not only the lack of detail on the Order-making power that is causing concern. The same applies to the detailed data retention notices served on individual CSPs. We understand that these would specify the CD each company will be required to retain and which may potentially be disclosed to the Agencies and other public bodies. Whether or not a particular CSP has been served a notice will remain confidential. This is understandable as this information would allow a criminal or terrorist to choose which CSP they use in order to avoid detection. The same holds true of the data sets to be retained which will be described in each CSP's notice (e.g. whether a company has, or has not, been obliged to retain location data for mobile telephones). It is clear to us that this level of detail must also remain secret.

53. In addition to the public concern at the lack of information in the Bill, we note that the CSPs are also seeking greater clarity as to the amount and type of CD they would be required to collect and retain under a data retention notice, how that will be decided, and the process for appealing if the CSPs and the Government cannot reach agreement.

- **We recognise that the draft Bill is deliberately broad in order both to permit future-proofing of the legislation against technological change and not to reveal gaps in operational capability. However, this is causing considerable concern for the Communications Service Providers, and also Parliament and the public. We therefore welcome the decision by the Home Office to make public information on the three core elements of the gap: subscriber details showing who is using an Internet Protocol address; data identifying which internet services or websites are being accessed; and data from overseas Communications Service Providers which provide services such as webmail and social networking to users in the UK. This is a positive step. However, we recommend that more thought is given as to whether this can be reflected on the face of the Bill.**

- **The data which would be most useful to criminals and terrorists, and which therefore is most sensitive, relates to the individual data retention notices. These must not be made public, since they would reveal which companies' services or applications can be used with the least risk of detection.**

(ii) Deep Packet Inspection and encryption

54. The Government clearly intends, wherever possible, to adopt a co-operative approach to obtaining CD from the CSPs. If the CSPs are unhappy with the contents of a notice, they can appeal to an independent body; the Government also has the ability to take civil action against an uncooperative CSP (we cover appeals at paragraph 68). In certain circumstances, the Government may decide that civil action is not appropriate. In such cases, it is important that there is an alternative means of accessing that CSP's data if the Agencies require it.

55. The solution the Government is proposing is to agree with the UK CSPs that they would place 'probes' on their network(s) to collect the required CD as it traverses to the end user. This is known as Deep Packet Inspection (DPI) technology. The Committee took detailed evidence on this, focusing on the feasibility of the technology. We heard that DPI is certainly not a new technology, and is in use for commercial purposes already. GCHQ told us that:

> *DPI is used pretty generally… [it's] a well-established technology. It's used by many Communications Service Providers in a range of ways, from network management to firewalls…*[35]

BAE Systems Detica – a supplier of DPI technology to the Government – confirmed this, and explained DPI's commercial applications in further detail:

> *You can also use [DPI] for other commercial purposes such as antivirus filtering, content filtering, parental controls. It gives you the ability to look at what is going on the network and make decisions about what you want to do with what's travelling on the network. So it's quite a flexible technology.*[36]

[35] *Oral Evidence – GCHQ, 18 October 2012.*
[36] *Oral Evidence – BAE Systems Detica, 17 October 2012.*

56. We questioned whether DPI is a technology that could be used successfully to extract CD from a data stream without intruding on the content of a communication. The Home Office, GCHQ and BAE Systems Detica were all confident that this was possible; ***. We were given an analogy regarding postal communications to explain how DPI works in this context:

> *So in this case [DPI] technology isn't programmed to look at the contents [of a communication]. It's just there to look at the communications data. So the analogy would be – and it's a bit simplistic, but bear with me – looking for the address on an envelope as opposed to looking at the contents of the letter… That genuinely is not difficult, [although those] protocols can change often. So you need to keep track of what the communications data fields are and how they sit within the overall communications stream.*[37]

57. We were also told by the Home Office that *** already operates DPI under the EU Data Retention Directive to collect CD.[38] Although this shows that the UK's approach is not new, the Home Office has accepted that it has a presentational issue to address in terms of the amount of DPI that may be used, what companies it may be targeted against, and how soon UK network CSPs may be asked to use it.

58. In public the CSPs have been unhappy about the concept of extracting CD from uncooperative overseas CSPs (i.e. 'third-party data'). Their opposition seems to be a mixture of principle and practicality – they would not wish to jeopardise their relationships with the overseas CSPs, and they believe it is for the overseas CSPs to release their own CD. In the evidence we took from the CSPs, however, their position was more nuanced. They said that their concern was over the extent to which the Home Office should attempt to negotiate with overseas CSPs before resorting to DPI. We were told:

> *… what we would expect is that there is proper due diligence conducted with those overseas service providers to see if the data that is required to be retained and disclosed is available… now, that's not specific in the Bill.*[39]

The CSPs, in short, wanted firmer reassurances (possibly even included on the face of the Bill) that they would only be requested to carry out DPI as a last resort.

59. The Committee has been told that DPI technology is most likely to be used where the Government cannot reach agreement with overseas CSPs: this is most likely to be the case in countries with which the UK has a more difficult relationship. GCHQ told us:

> *My view and understanding is that clearly the access strategy has to be linked to the areas that you really can't get the collaboration from *** as opposed to seeking that as your first route against people.*[40]

In these cases, we envisage that the UK-based CSPs will be more willing to undertake DPI.

- **It is important for the Agencies that there is some means of accessing communications data from uncooperative overseas Communications Service Providers. The Government's proposed solution appears capable of performing this role.**

---

[37] *Ibid.*
[38] *Written Evidence – Home Office, 22 June 2012.*
[39] *Oral Evidence – Communications Service Providers, 17 October 2012.*
[40] *Oral Evidence – GCHQ, 18 October 2012. ***.*

- **Whilst we recognise the UK Communications Service Providers' concerns, we believe they would be willing to co-operate in deploying Deep Packet Inspection technology. We are, however, sympathetic to their argument that the Home Office should have to demonstrate due diligence before resorting to the use of Deep Packet Inspection to collect communications data from overseas Communications Service Providers, and we recommend that this should be reflected on the face of the Bill.**

60. Another issue *** is that of the increasing encryption of communications. Witnesses at the Joint Committee have suggested that encryption will simply render DPI pointless. We have heard that the Government has *** options in dealing with the challenge encryption poses:

***.

61. ***.

- **We believe the Government has adopted a pragmatic approach to the issue of encrypted material. In the first instance, agreement should be sought with the Communications Service Provider holding the communications data to provide it in an unencrypted form.**

- **Where this is not possible, we accept that the only prudent alternative is to attempt to collect residual, unencrypted communications data associated with a communication, which – although of lesser volume – may nevertheless still be of intelligence value.**

(iii) The filtering tool

62. Given the increasingly fragmented nature of communications, with pieces of data relating to the same communication being held by different CSPs, CD requests are becoming increasingly complex. At present the Agencies may have to approach numerous CSPs and obtain sets of data which then need to be compared to find the information that is of use to an investigation. This can be laborious, time-consuming, and intrusive, with large amounts of data that are irrelevant to the investigation and that relate to innocent people being returned to the requesting officer.

63. The Government proposes in the draft Bill to establish a tool that will automate much of this process, gathering the data automatically upon authorisation of a request, and carrying out the analysis before returning only the useful result to the applicant. This will be quicker and, more importantly, will reduce intrusion into unconnected individuals.

64. We took evidence on the technical feasibility of establishing such a filter. The witnesses were agreed that the concept is theoretically possible, and both GCHQ and the Security Service use variations of such technology in their day-to-day business. GCHQ told us:

> *We already use in GCHQ similar sorts of technology that allow complex federated queries to be made from different data sources… so my sense is that it would be a challenge, but the underpinning technology is out there.*[41]

65. The complexity – and thus, uncertainty – comes from two areas: first, the number of different data sets held by different CSPs in different formats that will need to be brought together for the filtering tool to analyse and make sense of; and second, the differing

[41] *Oral Evidence – GCHQ, 18 October 2012.*

requirements of the various customers who will wish to use the tool, and how it can be designed to meet all of these. (The Security Service made reference to the SCOPE project, a failed IT system that was designed to link together all the security and law enforcement agencies, as an example of what can happen when such a range of customer requirements exists, although the Director General agreed that the filtering arrangements were not "*unfeasible*".[42])

66. The evidence we have taken suggests that the filter will have to be constructed on an incremental basis, with rigorous testing and validation at each stage. The Home Office appears to be working on a timescale of at least three years from the passage of the Bill until the filtering tool is operational. The new National Crime Agency (NCA) has been mentioned as a potential home for the tool, although the Home Office has said it would not wish to add to the NCA's responsibilities until the agency is fully operational.

67. The CSPs appear relaxed about the filtering tool, as from their point of view they are merely sending the information they currently provide to a different location. They did, however, raise a concern over whether material provided by the filtering tool could be constructed to an evidential standard: this is primarily a matter for the police and the courts rather than the intelligence and security Agencies and we have not, therefore, explored this issue further.

- **The ISC considers that a filtering mechanism would offer considerable benefits to the Agencies. It would save many hours of analysis, and reduce the amount of collateral intrusion from complex communications data requests.**

- **The technology seems to exist to provide this. It will be a significant challenge to integrate the numerous data sets from different Communications Service Providers to make the filter work, as well as to manage the expectations of the various departmental and Agency stakeholders. The record of government in managing such complex IT projects is mixed at best.**

[42] *Oral Evidence – Security Service, 17 October 2012.*

(iv) Other issues

68. We have considered the broader provisions of the draft Bill in order to establish context for those issues that directly impact on the Agencies. We have not covered them in any detail in this Report as they are, rightly, a matter for the Joint Committee. We do, however, make the following observations:

(i) Cost reimbursement: The Home Office has estimated that the cost of compensating the CSPs for complying with the Bill will amount to £859 million (of the overall £1.8 billion cost) over a ten-year period. However, there is little detail of the basis for this figure, which appears based on numerous assumptions:

What we've done is we've made certain assumptions in terms of the number of data retention stores we'll have to produce, certain assumptions in terms of, in extremis, if we have to put certain probes in place... we have made certain assumptions, for example that the cost of data retention will go down over time.[43]

We note that the Home Office is currently "*going through a process of revalidating the costs*"[44] associated with the Bill. However, it remains clear to us that there has as yet been no consultation with the CSPs, which must be involved in assessing what are, after all, their own costs:

Because we have no idea of how much we're going to be required to store, for example, [the cost] could be £1, it could be £5 billion… that estimate has been [made] with no consultation with us.[45]

More work is needed on costings and reimbursement arrangements, in consultation with the CSPs.

(ii) The appeals mechanism: The CSPs will, under the draft Bill, have the ability to refer their case to a body known as the Technical Advisory Board if they wish to contest the notice served on them.[46] We understand that the Technical Advisory Board will investigate the CSP's argument and report to the Home Secretary, although there is no obligation on Ministers to alter the notice on the Board's recommendation.

From our discussions with the CSPs, it is clear that there is an issue around remit (not all appeals will be around technical detail) and also around the lack of any real power being given to the Board:

The only right of appeal [against a notice] that we can see… is a judicial review, which is nonsense. So there needs to be something a bit more robust.[47]

Both these aspects of the appeals mechanisms must be strengthened to give the CSPs confidence in them.

[43] *Oral Evidence – Home Office, 16 October 2012.*
[44] *Ibid.*
[45] *Oral Evidence – Communications Service Providers, 17 October 2012.*
[46] *This was established under RIPA to hear appeals in relation to the lawful interception obligations.*
[47] *Oral Evidence – Communications Service Providers, 17 October 2012.*

AUTHORISATION PROCEDURES

69. The current process for applying for and authorising access to CD within the Security Service under RIPA comprises the following steps:

- Applicant determines that the purpose for which the CD is required is in line with one of the purposes set out in legislation – for the Agencies, this would be national security or another of their statutory functions.

- Applicant completes documentation setting out why acquisition of CD is necessary and proportionate to investigation, assesses likelihood of collateral intrusion into unconnected individuals, and considers the level of interference with the privacy of the subject of the request.

- Designated Authorising Officer (a middle manager at an equivalent grade to Inspector or Superintendent in a police force) reviews application and records their reasons for approving or rejecting the application.

- Single Point of Contact (responsible for liaison with CSPs) manages the process of obtaining the CD from the CSP and ensures that it is delivered to the Applicant, providing appropriate advice on applications and liaising with CSPs as required.

This process is subject to retrospective oversight by a team of independent inspectors reporting to the Interception of Communications Commissioner.

70. We have taken evidence from both the Security Service and GCHQ and it is apparent that this is a thorough and robust system, with the officers at each stage in the process being trained to a high standard to take their responsibilities seriously and reject any applications that do not meet the required thresholds. In particular, all applications must demonstrate that the CD is required for a purpose specified in RIPA and is connected to a specific operation.

71. This process is overseen by the Interception of Communications Commissioner, who conducts retrospective reviews of the arrangements in each Agency, examining previous applications for CD and making recommendations for improvements. We have heard evidence that the Commissioner has not identified any "*wilful or reckless*"[48] access to CD that would suggest that there are weaknesses in the systems in place that would allow unauthorised access to CD. It is clear to us that the Agencies take the Commissioner's inspections seriously, and respond promptly to any recommendations he makes for tightening up procedures. We understand that the Commissioner may be receiving a considerable increase in the number of staff and resources available in order to deal with the additional workload the Bill will impose on him.

72. These safeguards are not changing under the draft Bill. However, many of the Bill's critics argue that all requests for CD should be judicially authorised, as this would improve public confidence that applications were being independently scrutinised. The Government has introduced such a system for local authorities' applications, but these constitute only a small proportion of the overall total (0.4% in 2011). It is clear to us that the Interception of Communications Commissioner is not convinced that this will improve scrutiny: he has said this

[48] *Oral Evidence – Home Office, 16 October 2012.*

will only "*introduce unnecessary bureaucracy into the [authorisation] process and increase the costs associated with acquiring the data*".[49]

73. We have looked at what the effect of imposing such a system on the Agencies would be. They clearly feel that this would not be a positive step, and would affect their operational work. The Director General of the Security Service told us:

> *It would create many job opportunities for magistrates, because with *** authorisations a year, that would take a great deal of magisterial time. It would also be considerably slower, and the net effect of that, I think, would be that we would be much less able to take forward live investigations.*
>
> *If you are trying to pursue the activities of an individual or a group of individuals who are actively seeking to undertake a terrorist attack at some time in the future, then the ability to keep up with them in real time is absolutely critical, and I think it would be quite difficult to be confident that any judicial process would enable us to have that ability to keep up with the live real time actions of the targets.*[50]

74. The Director of GCHQ echoed the point:

> *If you're talking about GCHQ, I don't believe that a magistrate system could act with the tempo required, and I actually think it would provide less reassurance for a hardheaded committee once you actually looked at it.*[51]

- **The current arrangements within the intelligence and security Agencies for authorising communications data applications appear detailed and robust, and an appropriate safeguard on the use of these powers.**

- **Any move to introduce judicial oversight of the authorisation process could have a significant impact on the Agencies' operational work. It would also carry a financial cost. We are not convinced that such a move is justified in relation to the Agencies, and believe that retrospective review by the Interception of Communications Commissioner, who provides quasi-judicial oversight, is a sufficient safeguard.**

[49] *HC 496.*
[50] *Oral Evidence – Security Service, 17 October 2012.*
[51] *Oral Evidence – GCHQ, 18 October 2012.*

SUMMARY

75. Any proposals to intrude into the lives of citizens will, understandably, prove controversial and will, rightly, provoke debate. In the case of communications data, however, we accept that there is a serious problem that requires action.

76. The UK is not alone in facing the problem of the deteriorating access to communications data. We have held conversations with some of our 5-Eyes[52] counterparts who are clearly facing the same issues, as are our European allies. Some EU countries have cited the EU Data Retention Directive as the driver for change. However, the Directive does not impose any obligations on Communications Service Providers to retain data they do not need to hold for business purposes, and therefore cannot be used to address the 'capability gap'. The UK is amongst countries such as France and Denmark which have therefore chosen to take both a forward-looking and a transparent approach in seeking to introduce new legislation. In the classified version of the Report we sent to the Prime Minister, we included a summary of international comparisons. This contained a large amount of sensitive information, and so cannot be reproduced in the published version.

77. Our Inquiry has focused on the problem as it relates to the UK's intelligence and security Agencies: we reiterate that we do not see it as our role to form a judgement on the wider application of the draft Bill.

78. The Agencies require access to communications data – in certain tightly controlled circumstances and with appropriate authorisation – in the interests of national security. We recognise that changing technology means that the Agencies are unable to access all the communications data they need, that the problem is getting worse, and that action is needed now. We accept that legislation to update the current arrangements governing retention of communications data offers the most appropriate way forward.

79. Turning to the draft Bill, we strongly recommend that more thought is given to the level of detail that is included in the Bill, in particular in relation to the Order-making power. Whilst the Bill does need to be future-proofed to a certain extent, and we accept that it must not reveal operational capability, serious consideration must be given as to whether there is any room for manoeuvre on this point: Parliament and the public will require more information if they are to be convinced.

80. We have similar concerns regarding the background information accompanying the draft Bill. Whilst we recognise the need to take action quickly, the current proposals require further work. In particular, there seems to have been insufficient consultation with the Communications Service Providers on practical implementation, as well as a lack of coherent communication about the way in which communications data is used and the safeguards that will be in place. These points must be addressed in advance of the Bill being introduced.

[52] *The 5-Eyes countries are the UK, the US, Australia, Canada and New Zealand.*

THE INTELLIGENCE AND SECURITY COMMITTEE

The Rt. Hon. Sir Malcolm Rifkind, MP (Chairman)

The Rt. Hon. Hazel Blears, MP	*The Rt. Hon. Paul Goggins, MP*
The Rt. Hon. Lord Butler KG GCB CVO	*The Rt. Hon. George Howarth, MP*
The Rt. Hon. Sir Menzies Campbell CBE QC, MP	*Dr. Julian Lewis, MP*
Mr Mark Field, MP	*Lord Lothian QC PC*

The Intelligence and Security Committee (ISC) is an independent Committee established by the Intelligence Services Act 1994 to examine the policy, administration and expenditure of the three UK intelligence and security Agencies: the Security Service (MI5), the Secret Intelligence Service (MI6) and the Government Communications Headquarters (GCHQ). The Committee also examines the work of 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 Prime Minister appoints the ISC Members after considering nominations from Parliament and consulting with the Opposition. The Committee reports directly to the Prime Minister and through him to Parliament, by the publication of the Committee's reports. The Prime Minister may ask us to look into a matter, but most of the time we set our own agenda.

The Committee has an independent Secretariat currently hosted by the Cabinet Office. The Committee also has access to a General Investigator to undertake specific investigations covering the administration and policy of the Agencies; financial expertise from the National Audit Office; and a Legal Advisor to provide independent legal advice.

The Members of the Committee are subject to Section 1(1)(b) of the Official Secrets Act 1989 and are given access to highly classified material in carrying out their duties. The Committee holds evidence sessions with government Ministers and senior officials (for example, the Head of the Security Service). It also considers written evidence from the intelligence and security Agencies and relevant government departments. This evidence may be drawn from operational records, source reporting, and other sensitive intelligence, or it may be memoranda specifically written for the Committee.

The Prime Minister may publish the Committee's reports: the public versions have sensitive material that would damage national security blanked out ('redacted'). This is indicated by *** in the text. The intelligence and security Agencies may request the redaction of sensitive material in the report which would damage their work, for example by revealing their targets, methods, sources, or operational capabilities. The Committee considers these requests for redaction in considerable detail. 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 bare minimum of text is redacted from the report. We also believe that it is important that Parliament and the public should be able to see where we have had to redact information, rather than keeping this secret. Under the existing legislation the Prime Minister has the power to redact material without the Committee's consent, making a statement to that effect when he lays the report before Parliament. To date, this has never happened.

Published by TSO (The Stationery Office) and available from:

Online
www.tsoshop.co.uk

Mail, Telephone, Fax & E-mail
TSO
PO Box 29, Norwich NR3 1GN
Telephone orders/General enquiries: 0870 600 5522
Order through the Parliamentary Hotline Lo-Call: 0845 7 023474
Fax orders: 0870 600 5533
Email: customer.services@tso.co.uk
Textphone: 0870 240 3701

The Houses of Parliament Shop
12 Bridge Street, Parliament Square
London SW1A 2JX
Telephone orders: 020 7219 3890/General enquiries: 020 7219 3890
Fax orders: 020 7219 3866
Email: shop@parliament.uk
Internet: http://www.shop.parliament.uk

TSO@Blackwell and other accredited agents

ISBN 978-0-10-185142-8