**Graham Smith—supplementary written evidence (IPB0126)**

**ABOUT THE AUTHOR**


2. I have advised private sector clients on RIPA from time to time since its inception. I contributed to the discussion of DRIPA during its rapid passage through Parliament, primarily through an analysis of the draft DRIP Bill posted on my Cyberleagle blog. I made a submission to the Anderson Review (https://app.box.com/s/84t7w7b91ebstrn7qvvu1xoqrb5gb2r6).

3. This submission is made in my personal capacity. It should not be taken as representing the view of any client for whom I have acted or of Bird & Bird LLP, the firm in which I am a partner.

4. I have also submitted evidence to the House of Commons Science and Technology Committee¹, which I incorporate by reference.

5. I have set out below only those selected questions (in the general Call for Evidence and also specific questions indicated for my Oral Evidence session) to which I am providing a response. These represent only a small proportion of the issues raised by the draft Bill. For the most part I have concentrated on issues around clarity and scope of powers rather than debating the merits or otherwise of policies implemented in the draft Bill.

**RESPONSE TO GENERAL CALL FOR EVIDENCE**

**A. OVERARCHING/THEMATIC QUESTIONS**

**ARE THE POWERS SOUGHT WORKABLE AND CAREFULLY DEFINED?**

- **ARE THE TECHNOLOGICAL DEFINITIONS ACCURATE AND MEANINGFUL (E.G. CONTENT VS COMMUNICATIONS DATA, INTERNET CONNECTION RECORDS ETC.)?**

6. As will be seen from my responses to specific questions below, in some places there are significant problems with lack of clarity of definitions.

7. In some places (especially Internet Connection Records) critical terms that are not common currency or terms of art have been left undefined, leading to significant uncertainty as to their scope.

8. The Committee has heard evidence of the difficulty that the industry has had in correlating the definitions with actual datatypes held in, processed by or transmitted through their systems. If industry is experiencing difficulty, can the general public foresee with any degree of certainty the kinds of data that may be subject to retention, acquisition, interception or examination?

9. Definitions such as "Data" includes any information which is not data' surely invite comparisons with the impenetrability of RIPA.

- **DOES THE DRAFT BILL ADEQUATELY EXPLAIN THE TYPES OF ACTIVITY THAT COULD BE UNDERTAKEN UNDER THESE POWERS?**

10. The draft Bill is certainly a significant improvement on RIPA. For instance the arrangement whereby bulk interception warrants are set out in a separate section headed 'Bulk interception warrants' is far preferable to the reader having to hack through the impenetrable jungle of RIPA, chance upon Sections 8(4) and 16 and then have the insight to perceive that 'certificated warrants' are about bulk interception. The draft Bill is quite logically set out and it is generally explicit about the types of powers that it would grant.

11. However the draft Bill retains some of RIPA's vices. In respect of powers, chief among these is the obscurity of the apparently wide power to collect and examine related communications data as a by-product of bulk interception. In RIPA the potential extent of this power is revealed by chaining together collateral powers: metaphorically navigating the back alleys of the statute. For interception that arrangement has effectively been transposed into the draft Bill. (See further, response to Oral Evidence Question 16.)

12. The draft Bill also introduces some new problems of its own. These derive mainly from the definitional issues already mentioned. The definitions and intersections of various types of data – communications data, relevant communications data, related communications data, contents of a communication and so on – are difficult to conceptualise. The only realistic way to understand them is to test a list of real world examples against them and see which fall on which side of the various lines. The Home Office accompanying documents give a few examples, but not enough to test the definitions fully.

13. The Home Office could usefully produce a comprehensive list of datatype examples, where appropriate with explanations of context, categorised as to whether the Home Office believes that each would be entity data, events data, contents of a communication, data capable of being related communications data when extracted from the contents of a communication and so on.

14. A schedule of this type would inform the debate on this aspect of the draft Bill immeasurably. (In case it is of interest to the Committee, the batch of Snowden documents published by The Intercept in September 2015 contains an example of such a document.2)

15. Codes of Practice can helpfully include non-controversial illustrations of datatypes. However for reasons explained in my response to Oral Evidence Question 10 that is no substitute for a well formulated and intelligible statutory provision.

**Undefined terms**

16. Clause 47(4) uses the terms ‘internet service’ and ‘internet communications service’. Neither term is defined.

---

17. Presumably ‘internet communications service’ is intended to be narrower than ‘internet service’. However the draft Bill gives no indication as to where the dividing line between them may be. ‘Internet service’ does not appear to have previously been used in UK primary legislation. ‘Internet access service’, a more readily understandable term, has been used previously in both the Digital Economy Act 2010 and DRIPA.

18. ‘Internet communications service’ was used in DRIPA, where it was also undefined. That lack of definition may be because DRIPA replicated the 2009 Data Retention Regulations, which implemented the (now invalidated) EU Data Retention Directive. The Directive used the term ‘internet communications service’ but itself did not define it (see http://cyberleagle.blogspot.co.uk/2014/12/another-round-of-data-retention.html). It is not a term of art.

19. The Explanatory Note at para 120 refers to: “Identifying which communication services a person has been using, for example determining whether they are communicating through apps on their phone.” The implication may be that an “internet communications service” is intended to be restricted to messaging services – i.e. services by which human beings send each other messages (as opposed to, for instance, submitting search requests to a search engine) and to exclude automated device to server (or server to device) communication such as a software or data update.

20. That impression is reinforced by para 122 of the Explanatory Note: “In respect of purposes b. and c., the designated senior officer within a relevant public authority could only approve the application if it was to determine how an individual has been communicating with another individual online...”.

21. However paragraph 46 of the Guide to Powers and Safeguards refers to using ICRs to identify “services a suspect has accessed which could help in an investigation including, for example, mapping services”. The only clause 47 gateway that appears to be relevant to the example is 47(4)(b). That would not permit access to an ICR unless a mapping service were an ‘internet communications service’. That would give the term much wider scope than human to human messaging. If that is the intention, we have no clarity as to the actual width of ‘internet communications service’ or how it might differ from an ‘internet service’.

22. If, on the other hand, ‘internet communications service’ is intended to be limited to human to human messaging, the draft Bill does not make that clear. Nor, if that is intended, are we told how activities such as human to human messaging within online gaming services would be approached.

23. The meanings of 'internet service' and 'internet communications service' and the intended dividing line between them ought to be explained and articulated in the legislation.

**Is the wording sustainable in the light of rapidly evolving technologies and user behaviours?**

---

3 The current Data Retention Code of Practice attempts to provide an explanation. It says: ‘An internet communications service under DRIPA as amended by the CTSA is a communications service which takes place on the internet and can include internet telephony, internet email and instant messaging services.’
24. See next comments on future-proofing.

**OVERALL IS THE BILL FUTURE-PROOFED AS IT STANDS?**

25. Future-proofing has two sides. They are in tension with each other.

26. The first is to protect the powers against changes in technology, so that they are not rendered ineffective by new technologies falling outside the text of the legislation. Future-proofing in this sense leads to technology neutral drafting, which while gaining in terms of longevity tends to be abstract, difficult to understand and unclear as to how it applies to real world activities.

27. The second side to future-proofing is to ensure that the balance between intrusiveness and privacy settled upon by Parliament when it passes legislation of this kind is not thrown out of kilter by advances in technology. As technology reaches further into people’s lives, so technology-neutral powers will automatically follow. As the powers start to apply to unanticipated types of behaviour the consequences may be quite different from those envisaged by Parliament when it passed the legislation.

28. That has happened with RIPA. The combination of internet and mobile phone technology has, by a mere accident of technology, caught within RIPA’s net an ever-growing swathe of everyday activities and consequently thrown an avalanche of new data into the hands of law enforcement and the intelligence agencies. While the powers have remained the same, the balance between privacy and intrusion now embodied in RIPA bears little resemblance to that settled upon by Parliament in 2000. In that sense RIPA was anything but future-proofed.

29. Future-proofing of the second kind leans in the opposite direction from future-proofing of powers. It tends towards concrete, technology-specific drafting (and thus greater intelligibility), sunsetting of powers and frequent revisiting by Parliament (a) to ensure that the intended balance is maintained and (b) to consider any request to plug any gaps in powers that may have appeared.

30. Such a process also requires continuing information and openness about how the powers have been used, so that Parliament may engage in an informed debate when it comes to review the legislation.

31. Overall the draft Bill attempts to future-proof in the first sense, with predictable consequences of some very widely drawn powers and some relatively abstract and complex definitions. In my personal view the RIPA experience should teach us that this is undesirable and that the greater need is to future-proof whatever balance between intrusion and privacy Parliament decides to settle upon.

**B. SPECIFIC QUESTIONS:**

In that regard the various new non-disclosure provisions in the draft Bill give cause for concern. For instance the Home Office has publicly stated that the Clause 71 powers will be used to mandate the retention (or creation) of ICRs. However, as discussed in my oral evidence Clause 71 is far wider than that. If the use of Clause 71 were to be extended beyond ICRs in the future there appears to be no requirement on the Home Office to bring that to the attention of the public or Parliament, either before or after the event. Service providers would be bound not to reveal the content of the data retention notices by means of which such a change of policy was implemented.
COMMUNICATIONS DATA

- ARE THE DEFINITIONS OF CONTENT AND COMMUNICATIONS DATA (INCLUDING THE DISTINCTION BETWEEN ‘ENTITIES’ AND ‘EVENTS’) SUFFICIENTLY CLEAR AND PRACTICAL FOR THE PURPOSES OF ACCESSING SUCH DATA?

‘Content of a communication’ compared with RIPA.

32. RIPA has no definition of the content(s) of a communication. The meaning of ‘content’ underpins in RIPA (and will do under the draft Bill) not just the distinction between content and communications data for the purposes of warrants, data retention and acquisition notices, but also the scope of the interception offence and other provisions of the draft Bill. The clauses in which ‘content of the communication’ occurs include:

3(1)(b), 3(5): definition of interception

12(8), 106(8): extraction of related communications data from content of a communication (similarly 82(4) in relation to equipment interference, using similar definition of content in 82(4); and similarly 136(4) and 136(8); cf 149(2))

16(1): protection for MPs

33(2): lawful authority for interception by telecommunications service providers

45(1): definition of intercepted material

119(4): restrictions on examination of bulk intercepted material (both nature of material and purpose); similarly 147(4) for bulk equipment interference

121(1): definition of intercepted material

193(5): definition of communications data

33. The scope of the interception offence under RIPA has been the source of considerable uncertainty (see paragraphs 66 to 75 of my submission to the Anderson Review). Against such a fuzzy baseline it is difficult to say whether the new definition of content results in something much the same, broader or narrower.

34. However there are indications that it may be narrower. Chief among these is the omission from the draft Bill of any equivalent, for telecommunications, of S.2(5) RIPA.

35. S.2(5) provides that for both postal and telecommunications services interception does not include “conduct that takes place in relation only to so much of the communication as consists in traffic data comprised in … a communication … for the purposes of any … telecommunication system by means of which it is or may be transmitted”.

36. The draft Bill retains a corresponding provision for postal communications (for which no new definition of content is provided), but not for telecommunications. It may be that the new definition of content has narrowed the scope of interception sufficiently to render a saving for accessing traffic data superfluous. This may be the result of clause 196(6)(a) (see discussion at paras 46 to 47 below).

The definition of ‘content of a communication’
37. The framers of the draft Bill have the challenge of devising a definition that works as well for machine to machine communications as it does for person to person e-mails and messages.

38. This is a relevant consideration even without considering developments such as the internet of things. For instance when we access a website a series of background communications takes place between our web browser and the website server. Those messages are structured according to the HTTP protocol, with various sections and subsections. We have to be able to determine which of those sections contain content and which (if any) contain communications data (or, under the draft Bill's provisions for related communications data, contain data that would not be content when separated from the rest of the message).

39. The main part of the definition revolves around the ‘meaning of the communication’. If I send an e-mail, does this definition encompass only the message that I have composed and sent? Or does it also include the elements of that communication that mean something to the computers that will process them?

40. If the former, then large parts of most communications would not be content. Some parts might not be communications data either.

41. The latter seems more appropriate and likely, given the ubiquity of background machine to machine communications. However the definition then drives us to ask "For a computer to computer communication, what is the meaning of ‘meaning’?". Whether that is a good outcome deserves further consideration.

42. The definition of content is couched in terms of “what might reasonably be expected to be" the meaning of the communication. Crudely, if it looks like content, it is. If it doesn’t, it is not.

43. Thus the definition is framed from the perspective of the potential interceptor or retainer or acquirer of data, rather than from the perspective of the person whose communication it is. This is presumably intended to provide comfort to those making decisions about what type of authority is required to access the information.

Content, interception and data retention

44. The data retention provisions in Part 4 of the draft Bill do not, unlike the communications data acquisitions provisions of Part 3, exclude acts of interception from conduct that a data retention notice may require. On the other hand Clause 5(1) does not include data retention notices in the list of provisions that amount to lawful authority for interception.

45. Yet it seems that in order to create ICRs service providers may have to perform some interception-like activities in order to extract from transmissions some kinds of destination data (e.g. names of services).

46. Clause 193(6)(a) appears to prevent such activity being interception by excluding from content ‘anything in the context of web browsing which identifies the telecommunications service concerned’.
47. On the one hand this is highly technology-specific. It does not address any situations outside the context of web browsing (for instance a service accessed using a mobile app). On the other hand it excludes such data from content for all purposes in the draft Bill (see list in para 32 above).

Conclusion on definitions of content and communications data

48. The new definitions of content and communications data will fall to be applied within a wide variety of contexts.

49. It is difficult to propose alternative formulations without fully understanding what the Home Office intends should be the result of applying the definitions.

50. Given the significance of the definitions and the potential uncertainties about how they might apply it would be of considerable assistance if the Home Office were to produce a comprehensive list of examples as suggested above (paras 12 to 14).

DATA RETENTION

- **IS ACCESSING INTERNET CONNECTION RECORDS ESSENTIAL FOR THE PURPOSES OF IP RESOLUTION AND IDENTIFYING OF PERSONS OF INTEREST? ARE THERE ALTERNATIVE MECHANISMS? ARE THE PROPOSED SAFEGUARDS ON ACCESSING INTERNET CONNECTION RECORDS DATA APPROPRIATE?**

51. My comments are of necessity limited to a few impressions from reading the Operational Case for the Retention of ICRs without either specialist technical knowledge or operational expertise.

52. For Purpose 1 the Operational Case suggests that it is ‘likely’ that the matching process will identify a particular device as it is ‘unlikely’ that ‘many, if any’ of the other 5,000 devices using that IP address were accessing that email website in the same minute. (page 10).

53. The usefulness of this process appears to depend on the extent of the reduction that would be achieved by the matching process. A process that reduced 5,000 users to 1,000 would, presumably, be of little assistance.

54. The Operational Case could helpfully have provided more detail as to why a useful degree of reduction would be ‘likely’ as opposed to, say, a hope or possibility. The Committee has heard evidence about devices remaining continuously connected to particular services in order to receive notifications.

55. The Operational Case does not refer to the Danish experience of session logging, as to which written evidence has been provided to the House of Commons Science and Technology Committee. If the Home Office is proposing a different approach that could be expected to yield better results than the Danish experience, the Operational Case could usefully have indicated what that approach is and why it holds out the prospect of better results.

OVERSIGHT
Would the proposed Judicial Commission have sufficient powers, resources and independence to perform its role satisfactorily?

56. See response to oral evidence Question 8.

RESPONSE TO ORAL EVIDENCE QUESTIONS

(ORIGINAL NUMBERING)

OVERVIEW

Q.1. Aside from the new powers on the retention of internet connection records, does the draft Bill consolidate existing powers or does it extend them?

57. The draft Bill both consolidates existing powers and extends them. See my oral evidence and the detailed table in my evidence to the House Of Commons Science and Technology Committee.

58. In summary, leaving aside the question of whether explicit thematic, equipment interference and bulk data acquisition powers are or are not new:

Internet Connection Records

59. The additional communications data retention powers in Part 4 (clause 71) go far beyond Internet Connection Records, covering:

- Any type of human to human communication.
- Background activities of my smartphone when any app decides to communicate with a server – e.g. notification, data or software update.
- Any machine to machine communication – connected home thermostat, my car checking if it needs a software update, anything connected to the internet or any other network. In other words, the internet of things.

60. The above types of communication are all new compared with the current DRIPA schedule, which apart from internet access applies only to certain human to human messaging: internet e-mail, SMS messages and internet telephony. They also go beyond the amendments to DRIPA made by S.21 of the Counter-Terrorism and Security Act 2015 (IP address resolution).

61. Additionally:

- Inclusion of private services and systems is new (Cl.71(1) and 193(1)).
- The power in Clause 71 to require data to be generated for retention is new.

---

The current Data Retention Code of Practice sets out at paragraph 2.14 a list of IP address resolution datatypes which is identical to Clause 71(9)(a) to (e) of the draft Bill. However the way in which the list is used in each case is different. In the Code the listed items are given as illustrations of types of data that might be necessary to identify the IP address used by the sender or recipient of a communication, i.e. for IP address resolution purposes. In Clause 71(9) of the draft Bill the list is used in a reverse sense. It is presented as a self-standing list of things that ‘relevant’ communications data should be capable of identifying or assisting in identifying. That is far broader in scope than the usage in the Code, even assuming that the items in the Code list are in fact capable of assisting in the identification of the device or person using an IP address, which for most of the items on the list is not obvious.
The power in Clause 71 to require data to be obtained for retention is new (this point is additional to the points made in my oral evidence).

The current limitation to retention of data generated or processed in the UK is removed.

Technical capability notices (Cl 189)

62. Under RIPA (S.12) and the 2002 Maintenance of Interception Capability Order made under it notices may be issued to certain public service providers in order to require a technical capability to support interception. Under the draft Bill:

- For interception, technical capability notices are extended to private operators.
- The powers to issue technical capability notices in support of the targeted, thematic and bulk warrants under Parts 5 and 6 are new.
- The power to issue technical capability notices in support of acquisition of communications data under Part 3 is new.

Bulk interception

- A new power to treat some content as related communications data (108(8)).
- This is replicated for ‘equipment data’ in the new bulk acquisition and equipment interference powers

‘Telecommunications operators’

- The use of this new, broad, definition has a knock-on effect of expanding targeted and bulk interception powers

63. See also my separate discussion above of the new definitions of content and communications data, including whether they may have the effect of narrowing the scope of ‘interception’.

Oversight

Q.8. DO THE OVERSIGHT MECHANISMS IN THE DRAFT BILL SATISFY THE REQUIREMENTS OF ARTICLE 8 OF THE EUROPEAN CONVENTION ON HUMAN RIGHTS?

64. Under this heading I raise the question of secret legal interpretations.

65. Where powers are exercised or asserted on the basis of interpretations of statutory powers that are not made known to the public, the question could arise whether the requirement that the law be accessible to the public is satisfied. In any event, in terms of establishing public trust it would be desirable for there to be a mechanism whereby such interpretations are brought to public attention.

66. At present under RIPA this would only occur in the event of a complaint in the IPT or a legal challenge by a service provider against a warrant or notice. The position under the
draft Bill is similar. It contains, as far as I can discern, no mechanism to ensure that interpretations are proactively brought to public light.

67. That this is a real issue is illustrated by the Home Office’s interpretation of ‘external communications’ under RIPA, revealed in a witness statement of Charles Farr in the *Liberty* case in the IPT.

68. The background was that under RIPA S.8(4) GCHQ can intercept in bulk if its purpose is to intercept external communications. So the meaning of ‘external communications’ is significant.

69. The Home Office interpretation was controversial. It also had implications for who (or what) could be regarded as a sender or intended recipient of a communication, a basic building block of RIPA. (See further paragraphs 6.52 and 12.25 of A Question of Trust and paragraphs 31 to 54 of my submission to the Anderson Review.)

70. The Home Office’s interpretation, which underpinned the agencies’ operations under RIPA S.8(4) warrants, would not have seen the light of day had the NGOs not brought the IPT legal challenge. That occurred because of the Snowden disclosures.

71. Another example is provided by DRIPA. It was said that the DRIPA amendments to RIPA’s territoriality provisions and to the definition of telecommunications services did no more than reflect what the legislation had always meant. Those assertions were untestable, since the public had no way of knowing how the government might previously have interpreted the provisions either in the minds of its officials or in its previous dealings with communications service providers.

72. A similar issue could arise with the possible effect on end to end encryption of the draft Bill. This is a controversial topic, in its own right and also because Clause 189(4)(c) of the draft Bill can be compared with paragraph 10 of the Schedule to the 2002 Maintenance of Interception Capability Order (although the clause would apply in a much wider context, to a broader range of service providers and is drafted as an instance of a broader power). On the face of it at least some types of end to end encryption are applied not by a service provider but by the user. However the public is in no position to know whether the Home Office has previously adopted some other interpretation, nor (if the provision were to remain in its current form) what interpretations it might adopt in the future.

73. The draft Bill provides an opportunity to ensure that the proposed new oversight body proactively seeks out and brings to public attention material legal interpretations on the basis of which powers are exercised or asserted. Service providers might usefully also be able to bring a legal interpretation asserted against them to the attention of the oversight body, which would have to bring it to public attention. A procedure of this kind may be all the more necessary in the light of the new disclosure restrictions included in the draft Bill.

74. Such mechanisms would enable material legal interpretations to be publicly debated and if appropriate challenged. None of this would require to be made public any legal advice that the government had received, nor any factual matters that should properly remain secret, but only the substance of the legal interpretations themselves.
75. This would contribute to openness and transparency. By providing not only oversight but insight it would help to satisfy the requirement that the law should be foreseeable and accessible.

LEGAL PROFESSIONAL PRIVILEGE

Q.10 WHAT IS THE LEGAL STATUS OF THE CODES OF PRACTICE UNDER RIPA? WHAT DO YOU EXPECT TO BE CONTAINED IN THE CODES OF PRACTICE ISSUED UNDER THIS BILL?

76. Although the topic of Codes of Practice is raised here under LPP, it raises more general issues about the relationship between the text of the draft Bill and Codes of Practice.

Legal status of Codes of Practice

77. The legal status of Codes of Practice under the draft Bill is differently expressed from that under RIPA. S.72(4) RIPA assigns a general interpretative function (“relevant to any question arising in the proceedings... taken into account”) to Codes of Practice issued under S.71. This function is omitted from the draft Bill. Under the draft Bill (Schedule 6 para 7) Codes of Practice are generally admissible in evidence, but the only context specifically mentioned is a failure by a person to have regard to a Code.

Contents of Codes of Practice

78. The contents and quality of existing Codes of Practice vary. In some respects they can resemble an expanded set of Explanatory Notes. They are most useful and appropriate when fleshing out practice, processes and methodologies. The Interception and Communications Data Acquisition Codes of Practice are good examples.

79. Codes can also usefully provide uncontroversial illustrative examples. The Communications Data Acquisition Code has 5-6 helpful pages of explanation and examples of traffic data, subscriber data and service usage data.

80. It should not, however, be the role of Codes to fill substantive gaps in the parent statute, nor to interpret opaque or poorly drafted provisions of the parent statute. If the parent statute is clear and appropriately drafted, then the Code of Practice can follow suit. If the parent statute is muddled, opaque or obscure, the Code of Practice may compound the confusion and create controversy in its attempts to explain the statute.

81. It may be suggested that Codes of Practice can be used as a means of providing flexibility and thereby future-proofing powers granted by legislation against technological change. My own view is that this is not an appropriate use of Codes of Practice, for the reasons set out in the section on Future-Proofing. Even where Codes of Practice are required to be placed before Parliament they may not receive the scrutiny appropriate to what might, in effect, be updating legislation.

DATA RETENTION


Preliminary: ‘retention’
82. Current legislation (DRIPA, as amended by CTSA 2015) is limited to retention properly so called: retention of data already generated or processed in the United Kingdom by public telecommunications operators in the process of supplying the telecommunications services concerned.

83. Although the powers under Clause 71 are labelled ‘retention’ they go much further. Clause 71(8)(b) includes generation of data for retention and obtaining of data for retention. On their face these are both significant extensions over the existing data retention legislation.

84. It seems that Clause 71(8)(b) (a provision that approaches RIPA standards of impenetrability) could even be read as providing the power to require service providers to conduct 3rd party data retention. Presumably that is not the intention, since 3rd party data retention is an aspect of the draft Communications Data Bill that the government has disavowed.

85. Clause 71(8)(b) may perhaps also provide the power to require a service provider to require a third party, such its customer, to create data in order to provide it to the service provider.

86. If that is right, then could a data retention notice be used to require (say) the operator of a public Wi-Fi facility or an internet café to obtain and retain names and address details of its users? Some may think that would be a good thing. Others would deplore it. Either way, it does not seem right that a decision to impose an obligation of such significance could be made by way of a secret instruction of the Home Secretary based on an obscurely worded statutory power.

87. As to generation of data, the evidence of service providers to the Committee has suggested that ICRs do not exist as such on their systems. If they have to be created the power to require data to be generated assumes considerable significance.

Preliminary: essence of the right?

88. Question 14 is couched in terms of proportionality. However compulsory generation, obtaining and retention of communications data (in particular ICRs) may touch on a prior issue, namely whether the retention requirement respects the ‘essence of the right’.

89. Respect for the ‘essence of the right’ is explicitly recognised in Article 52 of the EU Charter.

90. The CJEU in Digital Rights Ireland considered whether the retention required by the EU Data Retention Directive violated the essence of the privacy right under Article 7 of the Charter. It held not:

“... even though the retention of data required by Directive 2006/24 constitutes a particularly serious interference with [Article 7] rights, it is not such as to adversely affect the essence of those rights given that ... the directive does not permit the acquisition of knowledge of the content of the electronic communications as such.”

ICRs and itemised phone bills
91. Destination data ICRs differ from the communications data considered in \textit{DRI}, in that arguably they may possess some of the qualities of content.

92. As well as affecting privacy rights mandatory retention of destination data ICRs would engage the right of freedom of expression.

93. This may seem a bold claim in the face of the oft-repeated assertion that ICRs are nothing more than the online equivalent of an itemised phone bill. The Home Secretary, introducing the draft Bill, said:

“So, if someone has visited a social media website, an Internet Connection Record will only show that they accessed that site, not the particular pages they looked at, who they communicated with, or what they said. It is simply the modern equivalent of an itemised phone bill.”

94. If a comparison can be drawn with an itemised phone bill, this would be an itemised phone bill like none ever seen\textsuperscript{6}. We can illustrate this by considering the questions that could be answered by scrutinising an actual itemised phone bill compared with one containing the destination information that would be logged in an ICR.

\textbf{Who has she spoken to?}

95. This is the focus of the traditional itemised phone bill.

96. The itemised phone bill shows called telephone numbers. In pre-online, pre-mobile days it would have been a fair assumption that whoever was using the telephone was speaking to somebody at the called number, so that a conversation took place\textsuperscript{7}. That might be somebody at a household telephone or at a public telephone box. The number might be a private office switchboard\textsuperscript{8}, at which point the information on the itemised phone bill terminated. It gave no information about which extension the call was routed to behind the private switchboard, or who took the call at that extension\textsuperscript{9}. (The former changed to an extent with the advent of DDI numbers.)

97. A subscriber lookup would provide information about the householder or organisation to whom the called number was allocated.

98. Itemised phone bills have always, with a few exceptions (e.g. dial-up data calls, recorded message services) essentially given information (including when the call was made and its duration) about conversations between human beings.

\textbf{What has she been doing?}

\textsuperscript{6} Nor should we forget that when itemised phone bills first appeared they excited alarm as to how revealing of people’s personal lives they could be.

\textsuperscript{7} Of course other possibilities existed, such as sending a coded signal by a pre-arranged sequence of calls and hang-ups. Nevertheless there was still a communication between two people.

\textsuperscript{8} The public telephone number of an office switchboard is somewhat equivalent in the internet world to an ISP allocating one public IPv4 address to the household or office router rather than allocating multiple public IPv4 addresses to individual devices in a household. An ISP allocating a public IPv4 address to one individual device in the household or office is a bit like what used to be called a ‘direct outside line’.

\textsuperscript{9} It is somewhat ironic that the example on page 9 of the ICR Operational case gives 4 digit extension numbers as an example of something equivalent to a port number. A private extension number would never appear on an itemised phone bill. An ‘extension’ would have appeared on a bill only if the caller dialled a direct line or a DDI number.
99. Our notional ICR itemised phone bill now starts to part company from an actual itemised phone bill. It is possible to infer a partial picture of someone’s activities by studying a record of whom she has talked to on the telephone. ICR logs differ in both degree and kind.

100. ICRs differ in degree in that we now speak on mobile phones and send text, e-mail, SMS and all the other varieties of messages to people in vastly greater volumes than we ever did in the days of landline telephone conversations. This itself provides a vastly richer and more detailed map of our activities than ever was possible with an itemised phone bill.

101. ICRs differ in kind from an itemised phone bill in that they are not limited to our conversations (whether voice, e-mail or messages) with other people. An ICR is an itemised phone bill that would log not just whom we conversed with when, but our online journeys: our 'visits' to the bank, the bookshop, the butcher, the baker, the travel agent, the doctor, the clinic, the hospital, the therapist, the support group, the hotel, the club, the concert hall, the public lecture, the political meeting, the trade union office, the ticket agency and so on without limit.

102. It would go further, logging not just our consciously initiated activities but also those initiated by our smartphones and connected tablets while they are in our pockets, beside our beds at night and so on.

103. In this respect ICRs bear little resemblance to an itemised phone bill. If anything they are more akin to universal CCTV surveillance when we step out beyond our front door and venture into public spaces. However that analogy is itself debatable.

What has she been reading?

104. ICRs would create logs of every website (or equivalent) that we accessed. On my understanding of the draft Bill that would include blogs and newspaper sites\(^\text{10}\).

105. In this regard ICRs are far removed from both itemised phone bills and CCTV in public places. They do not resemble any kind of log that it has been thought appropriate to compel in the offline world. It is as if, on our notional itemised phone bill, we were to find a state-mandated list of the titles of the books, newspapers and magazines that we had read in the last 12 months.

106. We never used to read books over the telephone. Now we read blogs remotely. It is a mere accident of technology that by doing that, instead of reading a physical book in an armchair at home, we engage in what the draft Bill (and RIPA before it) classifies as a 'communication'.

107. DRIPA was limited to something that people would generally regard as an online communication: internet e-mail, SMS messages and the like. Reading something remotely, however, is not a communication in the sense of a group of conspirators

\(^{10}\) The assumption in the draft Bill appears to be that all websites would be covered by ‘telecommunications service’ in Clause 47(6)(a) (see e.g. the Guide para 44). A scheme that required service providers subject to a retention notice to determine whether individual websites were or were not providing a ‘telecommunications service’ would presumably be unworkable. If a site were subject to retention under the (differently worded) Clause 71 but fell outside Clause 47(6)(a), then it would not be subject to the access restrictions of Clause 47(4).
discussing criminal plots between themselves. It is a highly personal activity of one individual alone.

108. Someone who accessed my own blog could\(^\text{11}\) trigger the creation of an ICR showing that they had accessed 'cyberleagle.blogspot.co.uk' (the URL up to the first slash), or maybe 'www.cyberleagle.com' if they used that address. The ICR might record the name of the blog: 'Cyberleagle'. It would record the date and time of the access\(^\text{12}\). It would presumably have to be linked at least to source data identifying (to the extent possible) the device that accessed the blog.

109. Mandating that logs of online reading habits be kept is analogous to being made, in the offline world, to keep a list of the books, newspapers and magazines that we have read in the last year.

**Privacy, freedom of expression and logging reading habits**

110. Reading is in the nature of a home activity. We are far more cautious about the intrusion of general powers into the home. We treat with greater respect for privacy activity takes place there than activity that takes place in public or semi-public places\(^\text{13}\). When considering online activities we should always consider whether the activity in question is an extension of the home or an excursion into a public or semi-public place.

111. State-mandated lists of reading habits also strike at the heart of freedom of expression. Our freedom to choose what to read is jealously protected for good reason. Reading fuels our quest for knowledge. It is emancipatory\(^\text{14}\). Merely making an officially mandated list of what we choose to read chills freedom of expression. If the ordinary citizen is put in the position of worrying about whether reading a controversial website might excite official suspicion or trip a red flag on some state computer system, that alone is sufficient to chill freedom of expression whatever the safeguards and restrictions on access.

112. A proposed law requiring us to make and keep a list of physical books, newspapers and magazines that we had read in the last 12 months could expect to be greeted with public outrage. This aspect of ICRs is an exact parallel.

113. Reading is also a large part of the 'online visiting' aspect of ICRs. The two are inextricably entangled.

114. Even if 'reading' websites could somehow be conceptually separated from 'visiting' websites, it is difficult to envisage any practicable way in which ICR retention could be implemented for only some types of website. Either way, the whole proposal would stand or fall with the 'reading' element.

---

\(^{11}\) If only the destination IP address were logged and not the blog's web address that might show only that the Blogger platform was accessed.

\(^{12}\) The ICRs Fact Sheet says: "[An ICR] will involve retention of a destination IP address but can also include a service name (e.g. Facebook or Google) or a web address (e.g. www.facebook.com or www.google.com) along with a time/date."

\(^{13}\) Red Lines and No Go Zones: the coming surveillance debate [http://cyberleagle.blogspot.co.uk/2015/07/red-lines-and-no-go-zones-coming.html](http://cyberleagle.blogspot.co.uk/2015/07/red-lines-and-no-go-zones-coming.html).

BULK INTERCEPTION WARRANTS

Q.16 SHOULD THE PRESENT POWERS RELATING TO BULK INTERCEPTION WARRANTS BE REPLICATED IN THE DRAFT BILL OR SHOULD WARRANTS BE MORE NARROWLY FOCUSED AS TO THEIR PURPOSE AND PERMITTED SEARCH CRITERIA?

115. The existing RIPA bulk interception warrant provisions have two distinct aspects: content and related communications data.

116. As to content, see my analysis of RIPA in ‘The tangled net of GCHQ’s fishing warrant’ (http://cyberleagle.blogspot.co.uk/2015/01/the-tangled-net-of-gchqs-fishing-warrant.html) The equivalent provisions in the draft Bill are generally similar, although the following are noteworthy in connection with points mentioned in my analysis:

- External communications are now replaced by overseas-related communications. While this governs the overall purpose of the interception, as with RIPA once communications (whether overseas-related or collaterally intercepted non-overseas-related) have been intercepted they form a common pool. No further distinction is made and there is no obligation (at least no express obligation) to identify and discard non-overseas-related communications.

- The draft Bill puts beyond any doubt (119(4)(a)) that for the purposes of selection for examination the relevant time for considering whether a person is within the British Islands is the time of the selection, not the time of the communication.

- The targeted examination warrant replaces the S16(3) modification.

- It is no clearer whether there is a dividing line between selection and examination, or whether examination can involve a continuing element of selection.

- The provisions regarding knowledge of a person’s location are similar, other than 119(3)(b) which removes the RIPA requirement that the belief that the selection prohibition would not be breached must be held on reasonable grounds.

- The S.8(4) certificate is replaced by ‘specified operational purposes’. Although the operational purposes cannot simply recite the statutory purposes (national security, prevention or detection of serious crime, national security-related UK economic well-being) they can still be general purposes (111(4)). (Curiously, the Home Office Guide refers throughout to ‘specific’ operational purposes.)

117. As to related communications data, appreciating the potential scope of this power remains (as with RIPA) a matter of chaining together collateral powers in a way that is not immediately obvious on the face of the statute.

118. This is one area in which it is no exaggeration to say that GCHQ collects all data (ISC Report March 2015, para 134):
119. A case could be made that a power of such potential reach (and the applicable restrictions on it) should be made clearer on the face of the statute. This power does not appear separately in the table of Powers at a Glance annexed to the Home Office Guide (I have prepared and annex a fuller version of the table).

120. Comparing the draft Bill with RIPA:

- Related communications data is made subject to ‘specified operational purposes’ (see above) rather than only being subject to the overall statutory purposes.

- The scope of the power is increased by the ability to treat communications data extracted from content as related communication data (106(8)).

- The structure of the RCD power is replicated (i.e. no British Islands selection restrictions) for bulk equipment interference ‘equipment data’ (136(4)). Similarly there is provision for equipment data extracted from content (147(8)). As with RCD the bulk communications data acquisition power (Part 6 Chapter 2) is not subject to any British Islands selection restrictions.

121. Given the far reaching potential scope of these powers it is pertinent to ask: How has the RCD power been used to date? How could the powers be used under the draft Bill?

122. There are three sources of information about how the RCD power has been used to date.

123. The first is the Interception Commissioner’s Report for 2014, published in March 2015. The Commissioner reported the results of its review of the use by agencies of (amongst other things) Related Communications Data. He said:

“6.63 Although my office’s investigation demonstrated that indiscriminate retention for long periods of unselected intercepted material (content) does not occur and the interception agencies delete intercepted material (if it is retained at all) after short periods, and in accordance with section 15(3) of RIPA 2000, I reported that related communications data are in some instances retained for a variety of longer periods and that I had yet to satisfy myself fully that some of the retention periods were justified.

6.64 This investigation led my office to make 22 specific recommendations in 2013 and 11 specific recommendations in 2014 for the interception agencies to review or shorten their retention periods and/or destroy intercepted material and/or related communications data where there was no persuasive justification provided for its ongoing retention. A number of the 2014 recommendations were to ensure that the interception agencies remained focused on the issue, to boost their efforts to review their retention periods or destroy certain material, and to create a corporate culture of

---

15 This assumes that data within 106(8) ceases to be content once extracted.
reviewing regularly and destroying material and data when it is no longer necessary and proportionate to retain it.

6.65 I can report that all of the recommendations were accepted by the interception agencies. The large majority have already been fully implemented. *This has caused a significant amount of intercepted material and related communications data to be destroyed, and in some instances entire systems have been decommissioned.* In other cases the maximum retention periods have been halved. Those agencies which have not yet managed to implement the recommendations in full are waiting on significant technical changes to be made to IT systems. I have made clear that future retention and destruction policies should not be dependent on broad assumptions about the value of the material or data. Reviews should be conducted regularly, informed by profiling exercises to ensure that the retention and destruction policies are not arbitrary. I welcome the progress made and my office will continue to monitor this area of the process.” (emphasis added)

124. The second source is the December 2014 judgment of the Investigatory Powers Tribunal in the *Liberty* case. The complainants argued that RIPA’s relatively loose restrictions on use of intercepted communications data could mean that, in the words of the Tribunal’s judgment:

> “a database can be built up of communications data (including communications data not excluded by s.16(2), as discussed above) so as to justify a continuing databank, continuously renewed by reference to the continued necessity for it for one of the s.5(3) purposes, not necessarily being the statutory purpose for which the communications data was originally intercepted.”

125. The Tribunal went on:

> “139. We are satisfied as a result of what we saw and heard at the closed hearings, and the further Disclosure set out above, that this is not the case and that there are adequate arrangements, in respect of duration of retention and destruction, to control and regulate the retention of such material. Such retention, storage and destruction policies and procedures are also regularly supervised by the Commissioner, as he makes clear in his Report.”

126. The government Disclosure referred to included the following passage:

> “As regards related communications data in particular, Sir Anthony May made a recommendation to those of the Intelligence Services that receive unanalysed intercepted material and related communications data from interception under a s8(4) warrant, and the interim Commissioner (Sir Paul Kennedy) has recently expressed himself to be content with the implementation of that recommendation.”

127. Exactly what this may mean in terms of the retention and use of RCD is not clear. However the value placed on it by the agencies is not in doubt. The ISC in its March 2015 Report said:

> “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 communication75 ***. 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.”

128. The government argued before the IPT that the absence of examination restrictions on RCD was justified by its use in order to determine whether someone was for the time being within the British Isles. This was necessary in order for the safeguard in Section 16(2)(a) to work properly:

“In other words, an important reason why the Intelligence Services need access to related communications data under the s.8(4) Regime is precisely so as to ensure that the s. 16 safeguard works properly and, insofar as possible, factors are not used at the selection that are - albeit not to the knowledge of the Intelligence Services - “referable to an individual who is ... for the time being in the British Islands”.” [112]

129. The IPT accepted that the different treatment of communications data “is justified and proportionate by virtue of the use of that communications data for the purpose of identifying the individuals whose intercepted material is to be protected by reference to s.16(2)(a).”[114]

130. The IPT rejected the NGOs’ argument that use of communications data for this purpose could be addressed by an exception in the legislation, saying that it was an “impossibly complicated or convoluted course”.

131. The third source, more controversially, is the batch of Snowden documents published by The Intercept in September 2015 (https://theintercept.com/2015/09/25/gchq-radio-porn-spies-track-web-users-online-identities/). These refer to various GCHQ events databases, including one called KARMA POLICE:

“KARMA POLICE aims to correlate every user visible to passive SIGINT with every website they visit, hence providing either (a) a web browsing profile for every visible user on the internet, or (b) a user profile for every visible website on the internet.”

132. ‘Visible to passive SIGINT’ appears to be a reference to bulk interception. There is mention of a prototype 17.8 billion row KARMA POLICE database representing 3 months’ data. As an events database (thus apparently containing no content) it can be assumed that KARMA POLICE would fall under the looser RCD examination regime.

133. Whether or not KARMA POLICE (or something like it) may exist today, a hypothetical KARMA POLICE is an interesting touchstone against which to test the draft Bill.

134. No doubt there will be differing views about whether it should be possible to use bulk warrants to build a hypothetical KARMA POLICE database, and if so whether the restrictions on the ability to search it should be tighter than the statutory purposes, specified operational purposes and necessity and proportionality.
135. But the prior question is would such a database be possible under the draft Bill? If so, given the new proposed ability to extract related communications data from content (corresponding to CDI as described in the ISC Report?), would a hypothetical “KARMA POLICE PLUS” be possible? Could such a database be fed from multiple sources (such as the communications data and equipment data product of bulk equipment interference and bulk communications data acquisition warrants)?

136. If nothing like this is intended to be possible, then the powers could and should be drawn more narrowly to reflect what is intended and to enable the debate to be framed accordingly. One question might be whether it is as impracticable as the IPT suggested to limit the use of RCD to identifying individuals who would qualify for the 'known to be within the British Islands' protection.

137. If the ability to build a hypothetical KARMA POLICE is intended, then the question arises whether it is appropriate for a universal database of internet browsing profiles (both domestic and foreign) to be capable of being built as a by-product of powers whose overall purpose is the interception of communications with an overseas element.

**Nothing to hide, nothing to fear**

138. RCD powers are a pertinent context in which to reflect on 'nothing to hide, nothing to fear'. It is a powerful slogan that strikes a chord with many, in the UK perhaps the majority of, people who are certain that we have nothing to fear from a benign state that is only trying to do its job to protect us: ‘GCHQ is welcome to read my e-mails any time they like. They won’t find anything to interest them.”

139. Many thousands of words, books indeed, have been devoted to counter-arguments. An immediate response, such as in a recent publication by the Open Rights Group (www.openrightsgroup.org/blog/2015/responding-to-nothing-to-hide-nothing-to-fear), is that even the most law abiding people have many legitimate reasons to keep things private. Whilst certainly true, that may cut little ice when you see the state as your trusty guardian angel: ‘Law enforcement has an important job to do. Only criminals could object. That’s not me.’

140. If an intelligence agency were to judge you only by what you said in your own texts and e-mails perhaps you could know that you have nothing to hide. (Although are you really sure that everything you have written was not open to misinterpretation? That you could always explain what someone else sent you? A modern day Cardinal Richelieu would have considerably more than six lines to work with.)

141. But a willingness to hand over your private life to a stranger misses the point that 21st century state surveillance is not just about our own lives. In a world of mass data capture and computerised analysis aimed at discovering new suspects it is as much about the company we keep, the places we visit and the patterns we weave online: our associations.

142. We may trust our online associates. But we cannot see inside their minds. We know little of their present, less of their past and nothing of their future. We know less than nothing about our associates’ associates.
143. In his report for 2013 Sir Anthony May, the then Interception of Communications Commissioner, sought to reassure the public that it has nothing to fear from GCHQ’s mass interception activities:

“I am, however, personally quite clear that any member of the public who does not associate with potential terrorists or serious criminals or individuals who are potentially involved in actions which could raise national security issues for the UK can be assured that none of the interception agencies which I inspect has the slightest interest in examining their emails, their phone or postal communications or their use of the internet, and they do not do so to any extent which could reasonably be regarded as significant.”

144. But how can any member of the public be certain that there is no ‘potential’ malefactor among their online associates? How can anyone know that they have nothing to hide, even from agencies acting with complete good faith and conscientiousness?
<table>
<thead>
<tr>
<th>Conduct authorised</th>
<th>Statutory bodies/purposes</th>
<th>Authorisation – Acquisition</th>
<th>Authorisation - Access</th>
<th>Oversight</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Targeted (13(1)) and Thematic (13(2))</strong></td>
<td><strong>Obtaining the content of a communication in the course of its transmission (12(2)(a))</strong>&lt;br&gt;<strong>Obtaining related communications data (RCD) from communications described in the warrant (12(2)(b))</strong>&lt;br&gt;Purposes: National Security, Serious Crime and Economic Well-Being of the UK (14(3))</td>
<td>Secretary of State authorisation, subject to approval by a Judicial Commissioner before non-urgent warrants come into force (14(1)(d))</td>
<td>N/A</td>
<td>Investigatory Powers Commission (IPC) replaces the Interception of Communications Commissioner Office (IOCCO), the Office of Surveillance Commissioners (OSC) and the Intelligence Services Commissioner (ISCom).</td>
</tr>
<tr>
<td><strong>Interception (14(1))</strong></td>
<td><strong>Obtain CD, usually via Communications Service Providers (CSPs) (46(2)) ('any person')</strong>&lt;br&gt;Public authorities provided with the ability to acquire CD and statutory purposes (46(7)) will be listed in the Bill.</td>
<td>Must be authorised by a designated person (who must be independent from the investigation) following consultation with a single point of contact (SPOC) (60). [Only the SPOC can approach CSPs to request CD] (??)</td>
<td>N/A</td>
<td>The judge-led IPC will have an extensive remit to oversee the use of all investigatory powers and will scrutinise those provided with</td>
</tr>
<tr>
<td><strong>Targeted (81(1)(a)) and Thematic (83(b)) Equipment Interference (EI)</strong></td>
<td>Obtaining private data covertly from computers and other equipment (communications, private information, equipment data – comms data, system data, extracted CD) (81, 82)</td>
<td>MI5, GCHQ, SIS, (84) law enforcement (89) and the Ministry of Defence (87)</td>
<td>Secretary of State authorises warrants for MOD and security and intelligence agencies. (84, 87) Chief Constable authorises law enforcement use. (89) All non-urgent warrants subject to Judicial Commissioner check before coming into force (84(1)(d), 87(1)(d), 89(1)(d)).</td>
<td>N/A</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td><strong>(lawful interception authority for stored communications only (5(1)(a)(ii), 81(6))</strong></td>
<td>MI5, GCHQ, SIS (107(1), 137(1)), 122(1).</td>
<td>Secretary of State authorises warrants, subject to approval by a Judicial Commissioner.</td>
<td>Examination of any material must be necessary for a specified Operational Purpose (which can be general (111(4)), 140(5)), 125(4)), authorised by a Secretary of State and approved by a Judicial Commissioner.</td>
<td>these powers though inspections, investigations, audits and authorisations of warrants and internal practices. Statutory Codes of Practice will outline further details.</td>
</tr>
<tr>
<td><strong>Bulk Powers</strong></td>
<td>Bulk interception (106) (obtaining content and related communications data (RCD) (106(4)(b), 106(5)(a)(ii)))</td>
<td>MI5, GCHQ, SIS (107(1), 137(1)), 122(1).</td>
<td>Secretary of State authorises warrants, subject to approval by a Judicial Commissioner.</td>
<td>Examination of any material must be necessary for a specified Operational Purpose (which can be general (111(4)), 140(5)), 125(4)), authorised by a Secretary of State and approved by a Judicial Commissioner.</td>
</tr>
<tr>
<td><strong>Bulk Equipment interference</strong></td>
<td>Warrants must be</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bulk Personal Datasets (BPD)</td>
<td>Additional safeguards for the acquisition and use of BPD</td>
<td>Authorisation to acquire particular classes of BPD issued by Secretary of State and subject to approval by a Judicial Commissioner</td>
<td>Examination of any material must be necessary for a specified Operational Purpose (153) (no provision saying may be general), authorised by a Secretary of</td>
<td></td>
</tr>
<tr>
<td>-----------------------------</td>
<td>--------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>(150)</td>
<td>MI5, GCHQ, SIS</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(135)(1)(b)</td>
<td>Obtaining private data covertly from computers and other equipment (communications, private information, <em>equipment data – comms data, system data, extracted CD</em>) (135, 136)</td>
<td>necessary in the interests of national security; may also be authorised for Serious Crime and Economic Well-Being (107(1)/(2), 137(1)/(2), 122(1)/2)</td>
<td>warrant.</td>
<td></td>
</tr>
<tr>
<td>Bulk acquisition of Communications data (122)</td>
<td></td>
<td>That requirement does not apply to:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Bulk interception: related communications data (because omitted from 119(1)(c))</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Bulk equipment interference: equipment data or non-content information connected with the equipment 147(1)(c), 147(8))</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Bulk acquisition of communications data, by its non-content nature</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>National Security Notices?</td>
<td></td>
<td></td>
<td>State and approved by a Judicial Commissioner.</td>
<td></td>
</tr>
<tr>
<td>----------------------------</td>
<td>----------------</td>
<td>----------------</td>
<td>-----------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Technical Capability Notices?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

22 December 2015