IN THE INVESTIGATORY POWERS TRIBUNAL **Case No. IPT/15/110/CH**

B E T W E E N:

PRIVACY INTERNATIONAL

Claimant

-and-

(1) SECRETARY OF STATE FOR FOREIGN AND COMMONWEALTH AFFAIRS

(2) SECRETARY OF STATE FOR THE HOME DEPARTMENT

(3) GOVERNMENT COMMUNICATIONS HEADQUARTERS

(4) SECURITY SERVICE

(5) SECRET INTELLIGENCE SERVICE

Respondents

CLAIMANT'S REPLY SKELETON ARGUMENT

For hearing commencing: Tuesday 26 July 2016

---

1. The Respondents' skeleton argument, despite its 119 pages, does not engage with the Claimant's pleaded case in key respects. The Claimant is therefore unable to make more than a few brief points in reply. It is hoped that the Respondents' reply skeleton will respond to the Claimant's actual case.

2. Two other issues arise:

    a. Sir Mark Waller's report has not been published. This is an unfortunate and serious error by the Respondents. The explanation offered is that "*a date was not confirmed for publication of the Intelligence Services Commissioner's report before the summer recess due to the exceptionally high volume of business following the change in Government. A date will be confirmed for publication in the autumn.*" However, the date for publication was arranged by reference to these proceedings and had been fixed well in advance. Despite the change in Prime Minister, HM Government made arrangements to lay other national security reports and papers before Parliament before the recess[1]. Laying a paper before Parliament is a routine exercise, not involving a vote.

    b. The Tribunal is invited to direct disclosure of the briefing given by the Security Service to members of the IPT, for the reasons given in correspondence. At the time of writing, it is unclear whether the Respondents object to disclosure.

[1] e.g. The newly appointed Home Secretary approved and laid the annual CONTEST report before the recess on 21 July; available at: https://www.gov.uk/government/publications/contest-uk-strategy-for-countering-terrorism-annual-report-for-2015.

Intrusiveness of BCD

3. An important overarching difficulty with the Respondents' position is the minimal weight they give to the seriousness and intrusiveness of BCD collection (see, for example, § 23 of their skeleton argument). The authorities cited at paragraph 8 of the Claimant's skeleton argument make clear that this approach is wrong. See, for example, the Advocate General's Opinion in *Watson & Ors* **[A3/63]** at § 259: '*The risks associated with access to communications data may be as great or even greater than those arising from access to the content of communications*'.

4. See also the recent academic study into the privacy properties of telephone metadata, which concluded that '*[t]he results of our study are unambiguous: there are significant privacy impacts associated with telephone metadata surveillance. Telephone metadata is densely interconnected, easily reidentifiable, and trivially gives rise to location, relationship, and sensitive inferences*' (Mayer, Mutchler & Mitchell, *Evaluating the privacy properties of telephone metadata*, PNAS 2016 113(20) at 5540).

5. Sir Anthony May commented in para 7.6 of his March 2015 Report **[A4/78]**:

> *The introduction of mobile phone networks with capacity to be able to provide access to radio & television channels, social networking and other services is staggering and so is the volume and detail of the data generated as a result, especially relating to the location of a mobile phone / end user device.*

6. These conclusions are hardly surprising given how modern life is lived in substantial part electronically and through communication devices, a fact further reflected in the enhanced and tightened test provided by *Szabo & Vissy v Hungary* [**A3/61**]. BCD provides:

    a. For those that *use* either landlines or mobile phones in the UK, a catalogue of whomever any individual has communicated with by voice or message;

    b. For those that *carry* mobile telephones in the UK, a catalogue of where everyone in the United Kingdom has been. By processing the date, one can identify with whom a particular phone owner has met (one off, recurrently), when and where; as well as with whom the user has communicated; and

    c. For those that that use the internet or internet-based apps, a catalogue of those corresponded with (by email, by social media) and of web domains (i.e. the web address to the "first slash") visited.

7. The intrusiveness of location data, that is just *one* sub-category of BCD, was summarised by Sotomayor J in the US Supreme Court in *US v Jones* at p. 3 (in a passage in a concurrence subsequently quoted by Roberts CJ for the Court in *Riley v California*):

> *GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations. See, e.g., People v. Weaver, ... ("Disclosed in [GPS] data . . . will be trips the indisputably private nature of which takes little imagination to conjure: trips to the psychiatrist, the plastic surgeon, the abortion*

clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on").

The Government can store such records and efficiently mine them for information years into the future ...

And because GPS monitoring is cheap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously, it evades the ordinary checks that constrain abusive law enforcement practices: "limited police resources and community hostility. …

8. Such a database of BCD is, for those living in or passing through the UK, complete: all communications with at least one party in the UK will generate BCD collected by s. 94 TA. It is precisely *because* it is unlawful to use a s. 8(4) RIPA warrant with the intention of getting a comprehensive dataset of internal UK BCD that s. 94 BCD has been used – it enables the Agencies to avoid the requirement that bulk collection have an external focus. This is what is obliquely expressed at §115 of the GCHQ witness statement **[CORE/B2/24]**.

9. In *Liberty v United Kingdom* (2009) 48 EHRR 1 **[A3/55]**, the Government informed the ECtHR that a 'broader approach' was required *only* in respect of communications outside the UK (at § 53):

> *… Within the United Kingdom the Government had extensive powers and resources to investigate individuals and organisations that might threaten the interests of national security or perpetrate serious crimes, and it was therefore feasible for the domestic interception regime to require individual addresses to be identified before interception could take place. Outside the jurisdiction, however, the ability of the Government to discover the identity and location of individuals and organisations which might represent a threat to national security was drastically reduced and a broader approach was needed. Maintaining operational effectiveness required not simply that the fact of interception be kept as secret as appropriate; it was also necessary to maintain a degree of secrecy as regards the methods by which such interception might be effected, to prevent the loss of important sources of information.*

This statement was made, even though the Government was aware that it was adopting exactly this 'broader approach' *within* the UK in relation to BCD (if not content), such power being exercised secretly through s. 94 TA. Such point applies with yet greater vigour in relation to the case put by the Government to this Tribunal in *Liberty/Privacy No. 1* **[A2/38]** when defending the collection of BCD without the safeguards provided by s. 16 RIPA and when defending the non-operation of the s. 16 RIPA safeguards in relation to BCD (see [111]-[114]). If the purpose identified by the IPT at [114] is indeed the purpose that explains and justifies the bulk retention of RIPA BCD, it is now plain from what is known about the combining of RIPA BCD and s. 94 TA BCD that, in very substantial part, such combined BCD are not intended solely for checking the location of a target, but rather as a freestanding investigative tool, a state of affairs which presents additional problems of legality and justification.

Issue 1: Section 94 under domestic law

(i) Consistency of the Respondents' Position

10. At §198 of the Respondents' Amended Open Response **[CORE/A2/45]**, the Respondents recognised that intercept, property interference or computer hacking all had to be authorised under the specialist statutory schemes and that s. 94 could not be used (emphasis added):

> *For the avoidance of doubt, no directions have ever been made under section 94 authorising the obtaining of the content of communications and/or the carrying out of equipment or property interference. The Respondents contend that such conduct can only be lawfully undertaken when authorised under the relevant provisions of (respectively) RIPA 2000, ISA 1994, and Part III of the Police Act 1997. …*

11. In their skeleton argument, however, the Respondents merely assert that sub-issues (b), (c) and (d) of the first issue (i.e. as to obtaining content of communications and carrying out equipment or property interference) '*do not … arise*' (§ 11). No explanation is given as to how the Respondents are able to reconcile their position in respect of communications content and equipment/property interference with their position in respect of communications data.

12. The Respondents' explanation cannot be found in s. 94 TA as it was initially enacted. The Respondents' analysis of s. 94 is that it confers a power of such breadth that it ought logically extend to communications content and equipment/property interference just as much as BCD.

13. Rather, as addressed at §55 of the Claimant's skeleton argument, the explanation missing from the Respondents' case is that such a conclusion can be rejected because there would be an impermissible circumvention of the subsequent specialist statutory schemes, enacted in IOCA 1985, ISA 1994 and PA 1997, if interception, property interference or computer hacking could be authorised under s. 94 TA. Those later specialist schemes confirm the narrow interpretation required by domestic law of the wide words of s.94 TA.

14. It thus remains impossible to fathom how as a matter of law the Respondents assert that:

    a. s. 94 TA is available to secure bulk collection of communications data notwithstanding that this enables circumvention of the specific statutory safeguards for obtaining such data put in place by RIPA ss. 8, 15 and 20 (i.e. it would be improper to seek a s. 8 warrant with the aim of obtaining the BCD of *internal* communications – s. 8(5)(a)) and by Part I Ch II (the safeguards for internal communications); but

    b. s. 94 TA cannot be used to secure collection of intercept of content, property interference or CNE. Clear words would be required to achieve this result, and there are later schemes with specific statutory safeguards.

    Why this inconsistent and inexplicable limitation is accepted is clear enough. Were it not made, the Government would have to accept that it had misled the ECtHR in each and every case in which the legality of the UK interception regime and its conformity with law was at issue.

(ii) Interpretation of s. 94

15. The Respondents argue that the Claimant seeks *'to remove swathes of power entirely'* from s. 94 (Respondents' skeleton argument, § 20). The construction advanced by the Claimant does not *remove* power, but rather asks the Tribunal to *interpret the legislation*, by reference to the power in its statutory context. There is nothing novel or unconstitutional about such proposition. Rather, what is clearly contrary to public law principles and authority is to construe a general power, not even referring to communications data, as permitting interference with fundamental privacy rights, or in such a way as to entirely subvert or circumvent a set of carefully crafted Parliamentary safeguards designed to ensure HRA/ECHR compliance in the specific case of taking of and access to communication data.

16. Ultimately, the process of reconciling general and specific statutory powers is a process of interpretation. As Laws LJ held in R (Cart) v Upper Tribunal [2009] EWHC 3052 (Admin) (at [36]-[38]):

> *The sense of the rule of law with which we are concerned rests in this principle, that statute law has to be mediated by an authoritative judicial source, independent both of the legislature which made the statute, the executive government which (in the usual case) procured its making, and the public body by which the statute is administered.*
>
> *The principle I have suggested has its genesis in the self-evident fact that legislation consists in texts. Often – and in every case of dispute or difficulty – the texts cannot speak for themselves. Unless their meaning is mediated to the public, they are only letters on a page. They have to be interpreted. The interpreter's role cannot be filled by the legislature or the executive: for in that case they or either of them would be judge in their own cause, with the ills of arbitrary government which that would entail. Nor, generally, can the interpreter be constituted by the public body which has to administer the relevant law: for in that case the decision-makers would write their own laws. The interpreter must be impartial, independent both of the legislature and of the persons affected by the texts' application, and authoritative – accepted as the last word, subject only to any appeal. Only a court can fulfil the role.*
>
> *If the meaning of statutory text is not controlled by such a judicial authority, it would at length be degraded to nothing more than a matter of opinion. Its scope and content would become muddied and unclear. Public bodies would not, by means of the judicial review jurisdiction, be kept within the confines of their powers prescribed by statute. The very effectiveness of statute law, Parliament's law, requires that none of these things happen. Accordingly, as it seems to me, the need for such an authoritative judicial source cannot be dispensed with by Parliament. This is not a denial of legislative sovereignty, but an affirmation of it …*

17. It is for the Tribunal, as the authoritative judicial source, to decide what the wide words of s. 94 TA means, in light of the safeguards that Parliament effected in RIPA.

18. As to the Respondents' assertion that the Claimant cites no authority for the proposition that it would be a misuse of power to circumvent more specific statutory safeguards (Respondents' skeleton argument, § 48), the Claimant relies on those authorities cited at § 61 of its skeleton argument. Further, in Secretary of State for the

Home Department v GG [2009] EWCA Civ 786 **[A2/37]**, the Court of Appeal considered the principle of legality, and the requirement for specific statutory wording to authorise infringement of fundamental rights; Dyson LJ held at [44]:

> *… general statutory words will not suffice to permit an invasion of fundamental rights unless it is clear from the whole statutory context that Parliament intended to achieve that result. If detailed provision has been made for the exercise of the general power, it may be possible to infer that Parliament intended the power to be exercised so as to infringe fundamental rights. That will depend on the precise provisions that have been made.*

It follows that, where '*detailed provision*' has been made to regulate the invasion of a right, it cannot be permissible, as the Respondents contend, to fall back on the '*general statutory words*' to authorise such conduct.

(iii) The proper use of s. 94 TA

19. At § 32 of their skeleton argument, the Respondents assert that, at the time the TA was enacted in 1984, the '*obvious use of the power*' was to collect bulk communications data, because there was no other statutory power for this purpose.

20. When the TA was given Royal Assent in April 1984, there was not (and could not have been) any suggestion that the purpose of the legislation was to respond to the decision in Malone v UK (1985) 7 EHRR 14 **[A3/46]**, judgment for which was not given until August 1984. Section 94 was not enacted to provide a statutory basis for the United Kingdom's interception or 'metering' of telephone communications. To the extent that § 32 of the Respondents' skeleton argument suggests otherwise, it is wrong. The true genesis of s. 94 TA had nothing whatever to do with BCD, as is demonstrated by the facts that:

    a. safeguards to address the deficiencies identified by the ECtHR in Malone were introduced only in the Interception of Communications Act 1985, rather than by modification of the terms of s. 94 TA. (It was not thought or suggested or argued that the deficiencies identified by Malone had already been addressed by the passage of s. 94 TA, which occurred after the facts at issue); and

    b. it was only in 1998 that GCHQ first used s. 94 TA to obtain BCD.

(iv) s. 22 RIPA

21. In suggesting that s. 94 TA and s. 22 RIPA are 'parallel regimes', the Respondents assert that 'international relations' is not a statutory purpose for which the s. 22 power could be used (§ 41, Respondents' skeleton argument). Such an argument overlooks s. 22(2)(h) RIPA, which provides as a relevant statutory purpose:

> *… any purpose (not falling within (a) to (g)) which is specified for the purposes of this subsection by an order made by the Secretary of State.*

22. The Secretary of State provided additional statutory purposes for s. 22 RIPA in Article 2 of the Regulation of Investigatory Powers (Communications Data) Order 2010 **[A15]**. There is no reason why the same power could not be exercised to extend s. 22 to cover 'international relations'.

23. Further, pursuant to the power contained in s. 25(3)-(4) RIPA, the Secretary of State can restrict the use of Chapter II of RIPA (provided that she complies with the requirement for public and democratic accountability via the positive resolution procedure in s. 25(5)). The Secretary of State is therefore able to control who can, and the circumstances in which they can, get access to communications data, for instance by inserting a requirement for consent to be sought and obtained from the Secretary of State.

24. In consequence, it is wrong to suggest that the scheme established by RIPA contains omissions in respect of access to communications data, which can only be filled by s.94 TA.

(v) Contrasting safeguards

25. The Respondents are concerned that the differences between the safeguards contained in the RIPA scheme and those contained in s. 94 TA are not '*overstated*' (§ 43(a), Respondents' skeleton argument). However, there is a significant disparity in safeguards. The diagrams in Appendix 2 provide a graphical representation of these stark differences.

Issues 2 and 3 – Article 8 ECHR

26. At present, there is little for the Claimant to say in reply. The Respondents have not engaged yet with the detail of the Claimant's case in its skeleton (or pleadings). In particular, they have not begun to address, whether in relation to BPD generally or BCD in particular:

    a. the criterion of 'strict necessity' which shapes the content and structure of any compatible safeguards against excessive discretion and arbitrariness: see ECtHR in *Szabo & Vissy v Hungary* **[A3/61]** at §§72-73;

    b. the requirement that BCD be used only for the specific purpose for which a strict necessity has been found, and thus, of necessity in the case of s. 94 BCD, only for national security reasons; or

    c. the plain requirement evident in *Szabo* for informed judicial authorisation and supervision (or its functional ilk) at key handling stages (acquisition, retention, sharing) as a required counterbalance for executive action and discretion: *Szabo* at §§75-78.

27. The Respondents' skeleton argument at § 66(a) advances the submission that the use of s. 94 TA to obtain BCD was foreseeable. This is entirely at odds with the factual evidence before the court:

    a. The collection of BCD under an aggressive interpretation of s. 94 was deliberately kept a closely guarded secret for over a decade in the case of the Security Service, and longer in relation to GCHQ (c. 17 years). There was no good reason to keep this fact secret if such use of s. 94 (or the potential for it) was foreseeable, especially given the Respondents' view that the same result could have been achieved (albeit after satisfaction of the RIPA safeguards) under RIPA.

    b. David Anderson QC in *A Question of Trust* explained that, at the time of his report, '*[t]here is nothing in the public domain concerning the use of [s. 94 TA] and*

the exercise of the s.94 power is not subject to any oversight or external supervision' (§ 6.17) **[A4/80]**. Indeed, one reason why Part I Chapter II RIPA powers were not used seems to have been that such would have triggered statutory oversight by the Commissioner, which, in all likelihood, would have led to avowal of such capabilities.

c. Through RIPA and the Codes of Practice, the Government made public its ability to obtain communications data under those mechanisms. Contrary to the Respondents' submission, most people would not assume that there was some additional, secret scheme with a much broader scope operating in the background, under which BCD was collected in precisely those cases where RIPA had chosen deliberately not to provide such power; and precisely in order to circumvent the safeguards provided by RIPA.

d. Such impression would be reinforced or confirmed by the consistent message provided by authoritative public sources such as White Papers or Ministerial statements in support of legislation, particularly RIPA and DRIPA (see Appendix 1).

28. At §§67-68 of the Respondents' skeleton argument, the Respondents rely on their rules, requirements or arrangements which are secret. Even if it is permissible to rely on entirely secret and (and 'unsignposted') arrangements, there must be sufficient information in the public domain to give citizens *'an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to this secret and potentially dangerous interference with the right to respect for private life'* (Malone **[A3/46]** at § 67). The Respondents' reliance on such arrangements prior to avowal of the BCD and BPD regimes is hopeless. The Tribunal is invited to rule consistently with its findings in *Liberty/Privacy No 2* **[A3/41]** at §§ 23 and 32: where there is insufficient information about the regime in the public domain, the regime contravenes Article 8 ECHR.

29. In any event, the Claimant does not accept that entirely secret programmes and arrangements interfering with a Convention right can meet the standard of foreseeability in Article 8(1). See Malone **[A3/46]** at §79.

30. The exercise at §§ 74-171 of the Respondents' skeleton argument is a 'tick-box', mechanical approach to the requirements set out in Weber. However:

a. Such an exercise is not sufficient, in the light of the ECtHR's clear indication in Szabo & Vissy v Hungary **[A3/61]** that the '*guarantees required by the extant Convention case-law on interception need to be enhanced*' (at §70); and

b. The Weber criteria themselves are not met, for the reasons explained in the Claimant's skeleton argument. The Respondents' skeleton argument does not address the serious problems with their conduct shown by the documents disclosed.

31. Further, in Liberty **[A2/38]** (at § 92) and Kennedy **[A3/59]** (at §§ 166-168), the oversight role performed by the Commissioner was afforded great weight. The Respondents similarly place weight on the important role performed by the Commissioners (Respondents' skeleton argument, § 68). But there was no formal oversight by the Commissioner at all in respect of BPD until the end of 2010, and there was no oversight of the necessity and proportionality of s. 94 directions until 2015. Such

informal oversight as occurred (for instance in 2004) was fundamentally deficient. Now that full oversight of s.94 has belatedly commenced (no doubt in part through the pressure of this litigation), a list has been produced by the Interception of Communications Commissioner of additional safeguards and improvements to the regime that are required **[A4/82/11-12]**. These remain in many respects unimplemented. Appendix 3 hereto contains a checklist of further matters identified by the Commissioner as a requirement of a lawful system, but as yet unaddressed.

32. The Respondents' submission that an entirely secret programme, collecting everyone's BCD and retaining it for at least a year, under an interpretation of a general power whose operation in this way was secret for 17 years, with no public safeguards and no oversight, is and always was '*in accordance with law*' is extraordinary and wrong. As in *Belhaj* **[A3/42]**, the Respondents ought to accept the inevitable.

THOMAS DE LA MARE QC

BEN JAFFEY

DANIEL CASHMAN

Blackstone Chambers

25 July 2016

Appendices:

1 – Statutory Purpose Material
2 – Diagrams of Safeguards
3 – IOCCO's analysis
4 – Claimant's schedule cross-referenced to the main skeleton

A referenced Chronology is also provided as a guide through the materials.

Appendix 1 – Statutory Purpose Material

Emphasis added in bold and underline

RIPA 2000

***Interception of Communications in the United Kingdom: A consultation paper,* CM 4368, June 1999**[1]

Page	Extracted Text of White Paper
1	This Consultation Paper sets out the Government's proposals for reforming the legislation which governs the interception of communications in the United Kingdom. The proposed changes are designed to: (a) update the legislation to take account of communications services introduced since the existing legislation was enacted (b) extend the law to cover interception of private telephone networks (c) **provide a clear, statutory framework for authorising the disclosure of data held by communications service providers** (d) retain the existing safeguards which ensure that interception is authorised only when it is justified in relation to strict statutory criteria, and that the use of the power is subject to independent judicial oversight. … The Government is committed to ensuring that interception of communications complies fully with the ECHR, and this paper describes the separate frameworks for authorisation, oversight and redress with which we propose to achieve this.
3	The legislation will provide a clear framework governing the interception of private networks, setting out the circumstances in which it may be authorised and the safeguards which should apply. The Government believes that the law surrounding access to communications data is in need of revision. Itemised billing, for example, can be of tremendous investigative value, and it is right that in certain circumstances the authorities should be able to access this material. However, it also involves a measure of intrusion into individual privacy and **it is essential that access should be carefully controlled in accordance with ECHR proportionality requirements, authorisation only being given where necessary and justified for clearly defined purposes. For these reasons we are proposing to establish a clear, statutory framework for access to communications data**.
16	4.1 The intention is to provide a single legal framework which deals with all interception of communications in the United Kingdom, regardless of the means of communication, how it is licensed or at which point on the route of the communication it is intercepted. This means that the scope of the Bill will be wider than that of the Interception of Communications Act 1985 (IOCA) in three specific areas; non-public networks, wireless telegraphy and interception of mail.

[1] http://webarchive.nationalarchives.gov.uk/20100418065544/http:/homeoffice.gov.uk/documents/cons-

	… 4.5 The Government believes that it should not make any difference how a communication is sent, whether by a public or non-public telecommunication or mail system, by wireless telegraphy or any other communication system. Nor should the form of the communication make any difference; all interception which would breach Article 8 rights, whether by telephone, fax, e-mail or letter, should all be treated the same way in law. A single authorising framework for all forms of lawful interception of communications will mean that each application will follow the same laid down procedure and will be judged against a single set of criteria. This will ensure that this type of intrusive activity is used only when justified, necessary and, in the case of criminal investigations, proportional to the offence.
26	Chapter 10 – Provision of Communications Data … 10.3 In recent years, advances in telecommunications have meant that the amount of data held by communications service providers has increased, making the information much more useful as an investigative tool. But so has the potential for privacy infringements. Although accessing a person's communications data is not as intrusive as interception, it clearly still represents an interference with the privacy of the individual. **The Government therefore believes it is time to put in place a statutory framework for authorising access to communications data.** 10.4 **The Government proposes to introduce a statutorily based framework to regulate access to communications data by investigating bodies**. This will lay down the purposes for which an application for access to communications data may be made, the minimum standards of information which must be included within an application and the factors which must be taken into account by the authorising official. We also propose to introduce strict statutory requirements regarding the handling, storage and retention of communications data. It is intended that these measures will be laid out in detail in the publicly available Code of Practice (see paragraph 7.16). 10.5 The proposed purposes for which data access may be authorised are: (a) for the prevention or detection of crime; (b) for the apprehension or prosecution of offenders; (c) in the interests of national security; (d) for the purpose of safeguarding the economic well-being of the United Kingdom; (e) for the urgent prevention of injury or damage to health; and (f) for the assessment or collection of any tax or duty or of any imposition of a similar nature. 10.6 Where a request has been properly authorised in accordance with the arrangements outlined above, the communications service provider will be required to provide the specified material within a reasonable period.

Hansard

Commons, Second Reading: HC Deb 06 March 2000 vol 345 cc767-835[2]

Mr Straw	Chapter II of part I deals with the acquisition of communications data, which are normally provided to investigating bodies under a voluntary regime set up by the Telecommunications Act 1984 and the Data Protection Act 1998. **This existing and loosely regulated regime is unacceptable in terms of human rights and because, in certain cases, it has led to unacceptably high demands on the public telecommunications operators.** **The Bill sets out in statute precisely what hurdles law enforcement and other agencies must overcome before they can require the data from service providers.** The Bill then puts an onus on service providers to provide the information, and allows for them to be compensated—a proper statutory regime which is much to their benefit.
Mr Beith	Communications data cover the acquisition of information about telephone numbers that are being dialled from a specific telephone and the location from which a mobile telephone is being used. That is not the same as listening to the conversation on those phones. I can accept that that represents a lower level of intrusion and it has rightly been brought into the Bill's ambit to provide some protection and regulation. However, in Committee **we must consider whether the lower levels of authorisation are adequate for citizen protection and, indeed, whether they meet the European convention on human rights requirement, which is the basis of much of the Bill. If not, we are wasting our time enacting them in this form**.

Written Answers: HC Deb 19 April 2000 vol 348 c509W[3]

Mr Cohen	To ask the Secretary of State for the Home Department if he will make a statement on his policy in respect of the use his Department, its agencies and public bodies will make of the powers relating to the authorised obtaining of communications data in Part I, Chapter II of the Regulation of Investigatory Powers Bill once the Bill is enacted.
Mr Straw	**Part I, Chapter II** of the Regulation of Investigatory Powers Bill **provides** the law enforcement, **security and intelligence agencies with the power to require communications data**, such as subscriber details and itemised billing, **in a closely controlled manner** and for a number of specific purposes such as preventing or detecting crime. **The Bill provides greater safeguards** than those which are currently in place for the provision of such data under the Data Protection Act regime, but the purposes for which it may be obtained under the new legislation are very similar. As a result, I do not expect any significant change in the extent to which communications data are obtained.

[2] http://hansard.millbanksystems.com/commons/2000/mar/06/regulation-of-investigatory-powers-bill#S6CV0345P0_20000306_HOC_199

[3] http://hansard.millbanksystems.com/written_answers/2000/apr/19/regulation-of-investigatory-powers-bill-1#S6CV0348P0_20000419_CWA_143

Lords, Second Reading: HL Deb 25 May 2000 vol 613 cc880-913[4]

Lord Bassam	The second power regulated in the Bill provides for access to communications data. Law enforcement and other agencies routinely use communications data in a variety of investigations. At present, they are handed over voluntarily by service providers under the Data Protection Act. **The Bill introduces a new regime which requires the requesting agency to go through a number of checks before it can make a request of a service provider.** A subsequent audit of the requests will be carried out under the auspices of the Interception of Communications Commissioner, who will report annually to the Prime Minister.
Lord Lucas	Secondly, we need to look at the area of communications data. At the moment, of course one understands that the police want access to people's telephone bills. The question of who a person has been telephoning, of who has phoned you and when, has been an aspect of detective fiction for as long as I can remember. But this will become much more universal. Looking 10 years ahead, I would expect to be conducting most of my life electronically. Everything that I have done in every aspect of my life will be recorded in communications data. **We need to make sure that when someone is getting access to that. they do so in a way which is proper, authorised and consistent with the general liberty of the citizen. I think it is possible that the Bill is drafted correctly in that respect**. I do not necessarily share the doubts that have been expressed, but it is something we shall have to look at with great care.

Lords Committee: HL Deb 19 June 2000 vol 614 cc97-146[5]

Lord Bassam	The difference between accessing communications data and interception can be equated to the difference between directed surveillance and intrusive surveillance. **Although communications data have been accessed for many years under a variety of statutes, this is the first time that the Government have sought to place these arrangements on a clear and specific statutory basis.** **The effect of this part of the Bill will be to provide far greater accountability, oversight and safeguards—something we all wish to see—for accessing this type of data than has previously been the case**. Furthermore, it will be done in a manner that will work in an operational context. **…** I now turn to Amendments Nos. 74A and 75A and to the more precise detail. While it is right that **the Bill will provide a much better statutory framework for accessing communications data than the arrangements that currently exist**, there are circumstances in which access to material may not be possible under the Bill, yet the person requiring the data may have a quite legitimate claim. For instance, communications data is sometimes required by defendants in criminal proceedings when they feel that it would assist their case. They obtain the data under a **judicially authorised** production order. That is the route that international requests normally follow. So while the vast majority of communications data will be supplied under these arrangements,

[4] http://hansard.millbanksystems.com/lords/2000/may/25/regulation-of-investigatory-powers-bill#S5LV0613P0_20000525_HOL_72

[5] http://hansard.millbanksystems.com/lords/2000/jun/19/regulation-of-investigatory-powers-bill-2

	there will be some exceptions for which the Bill does not cater. There will also be cases where communications data, like any other document or piece of information, can be obtained compulsorily by bodies with their own compulsory powers. However, it may reassure the noble Lord to know that, since the arrangements under the Data Protection Act are voluntary, **holders of communications data will be quite within their rights to refuse to supply under the Data Protection Act and to insist that the strict controls imposed by the Bill are, instead, adhered to**. They would, of course, still be obliged to supply communications data in response to a judicially authorised production order. … In our earlier discussion, I tried to outline how we saw communications data. However, I shall reflect further on the matter. We see the communications data definition as having three essential elements: first, it addresses information—that is, who a person is communicating with; secondly, it deals with usage of information—how long calls last, the time that the call was made, and so on; and, thirdly, it deals with any other information that may be held about a customer by a communication service provider. I believe that those are the three essential elements. If we were to agree Amendment No. 76, all those elements would be removed. However, I know that that is not the noble Lord's intention. But we are insistent—a feeling which I believe is shared by us all—that **we need to have an effective definition. Without it, we would probably be in breach of the European Convention on Human Rights. That convention demands clear legal limits on what kind of data can be obtained in this way. For that reason, we think that it is better to provide a definition of "communications data"**. … The framework introduced in this Bill reinforces all the useful work which has already taken place and **places it on a firm statutory footing**. It removes the liability which suppliers of communications data had under the Data Protection Act and places it on the agency requiring the data instead. **It provides a clear independent oversight mechanism which never existed previously. And people will be able to complain to the regulation of investigatory powers tribunal if they believe that their communications data has been accessed improperly**. For those reasons the Bill will improve current arrangements. [Revised definition of 'communications data' proposed on 12 July 2000][6]

[6] http://hansard.millbanksystems.com/lords/2000/jul/12/regulation-of-investigatory-powers-bill

DRIPA 2014

Hansard

Commons Second Reading: 15 July 2014[7]

Theresa May	In my statement to the House last Thursday, I made clear **the urgent need for narrow and limited legislation on communications data and interception**. There is no greater duty for a Government than the protection and security of their citizens when we face the very real and serious prospect that the police, law enforcement agencies and the security and intelligence agencies will lose vital capabilities that they need in order to do their jobs. Communications data—the "who, where, when and how" of a communication, but not its content—and interception, which provides the legal power to acquire the content of a communication, are crucial to fighting crime, protecting children, and combating terrorism. … The ECJ ruling in April was critical of the data retention directive because it said it did not contain the necessary safeguards in relation to retained data. I said that to the House last week and referred to it earlier this afternoon. Of course that ruling did not take into account the different structures, regimes and domestic laws that are in place in individual member states. **Our communications data access regime, primarily governed by RIPA, has strict controls and safeguards in place. The data can only be accessed when it is necessary and proportionate for a specific investigation, and access is limited and subject to a strict authorisation regime, which was specifically endorsed by the Joint Committee on the draft Communications Data Bill.** Clause 3 provides an important clarification in that it makes it clear that the statutory purpose of safeguarding the economic well-being of the UK can only occur when it is in the interests of national security. That is already the position, but the Bill puts that position beyond doubt. … Alongside the legislation, of which I have stressed the urgency and importance, it is right that we balance the use of sensitive powers against the public's right to privacy. I have detailed **the limits on access to communications data** and interception that will be enshrined in the primary legislation. In addition, I announced last week a package of measures to strengthen safeguards and to reassure the public that their rights to security and privacy are equally protected. We will reduce the number of public authorities able to access communications data. We will establish a privacy and civil liberties oversight board. We will appoint a senior former diplomat to lead discussions with other Governments on how we share data for law enforcement and intelligence purposes. We will also publish an annual transparency report on the use of sensitive powers. … As I made absolutely clear last week, the Bill merely preserves the status quo. It does not extend or create any powers, rights to access or obligations on communications companies that go beyond those that already exist. It does not address the same problems or replicate the content of the draft Communications Data Bill, published in 2012. The use of modern technology and changes in how people communicate have **caused a decline in**

[7] http://www.publications.parliament.uk/pa/cm201415/cmhansrd/cm140715/debtext/140715-0002.htm#14071547000001

	our ability to obtain the communications data that we need. I continue to believe that the measures contained in the draft Communications Data Bill are necessary to bridge that gap, but that is emphatically not what we are considering today. Parliament will need to return to those issues following the general election. The review to be undertaken by David Anderson, to which I have just referred, will consider the issue and I hope it will inform the debate.
Yvette Cooper	My understanding is that **the Government do not keep metadata on UK citizens** and that the data retention directive is about the information that companies hold, but I would certainly be very surprised if companies were able to separate out the billing data for MPs, for example, from that of any other British citizen. It would be startling if they were able to do so. My hon. Friend is right that one would expect things such as the data retention directive to cover not just MPs but all UK citizens in that way, but my point is that the Government cannot take for granted the need to restore the status quo. We need to debate it and we need reform. … The Government have rightly made changes to ensure that the new legislation can comply with the ECJ directive. They have narrowed the number of organisations that can access the data, for example, and **introduced further safeguards to ensure that the process is necessary and proportionate**.
David Davis	Much of this failure hinges on the fact that access to communication data in this country is not subject to judicial approval. It is one of the differences between ourselves and America and some other European countries. It is approved by officers of the same organisation that request it. The result of that—the point that I think the hon. Member for Brighton, Pavilion (Caroline Lucas) was referring to—is that too many people have too much access, too easily, to too much data. That is the core point. Therefore, we use this power in that respect more often than many of our international colleagues.
Jack Straw	The telephone tapping that happened to me and my family was the subject of no statutory warrant whatsoever. The past 30 years have seen this House progressively doing its duty by the citizen—from the Telecommunications Act 1984 and the Intelligence Services Act 1994 through to, I am proud to say, the Human Rights Act 1998 and the Regulation of Investigatory Powers Act 2000—to ensure that the necessary powers of the state to detect and prevent crime and to secure national safety are the subject of proper controls. Of course, as technology changes, the law should take account of it—both sides of the House are agreed on that—but **RIPA was a huge advance in terms of human rights, and that was how I introduced it to the House back in 2000**. … **Before the Telecommunications Act 1984 and the Intelligence Services Act 1994, data communications of all sorts were collected without any statutory control. That, too, has been the subject of repeated strengthening of the law, to protect the citizen.** I hope this House will pass this sensible, necessary and very modest measure.

Commons Committee: 15 July 2014[8]

James Brokenshire	Obviously, we have considered carefully the impact of the European Court of Justice judgment, the European convention on human rights and other parts of the law in examining the position. That is why we have considered the Bill so carefully. **The additional safeguards and provisions that have been written into the Bill reflect that consideration**. We remain confident that the provisions meet the legislative requirements. … Given that the European Court was considering only the data retention directive and not how member states implemented it, it did not take into account **the rigorous controls in place in the UK as part of its judgment. Access to communications data in the UK is stringently regulated and safeguarded by the Regulatory and Investigatory Powers Act 2000. Data are retained on a case-by-case basis and must be authorised by a senior officer, at a rank stipulated by Parliament, from the organisation requesting the data. The authorising officer may approve a request for communications data only if the tests of necessity and proportionality are met in the particular case.** Our system was examined in detail by the Joint Committee on the draft Communications Data Bill, and it was satisfied that the current internal authorisation procedure is the right model. However, **to ensure that communications data cannot be accessed using information-gathering powers that are not subject to the rigorous safeguards in RIPA, the Bill ensures that data retained under this legislation may be accessed only in accordance with RIPA, a court order or other judicial authorisation or warrant**.
Sir Alan Beith	It is important that we make it absolutely clear that **we have a set of rules** to ensure that **the Government only require the retention of data when they have good purpose for doing so**, and they only retain those kinds of data for which there is good purpose. **Access to that data should be the subject of stringent conditions**. In essence, that was what the European Court judgment was about, and **the Government are meeting those conditions in the way that they have framed this legislation**.
Jack Straw	I will deal first with the point made by the hon. Member for Cambridge (Dr Huppert) and others about the Regulation of Investigatory Powers Act 2000. I was the Minister responsible for RIPA. It was a carefully constructed Act that was preceded in 1999 by a lengthy consultation process. Everybody recognised at the time that it was a major improvement on the legislative regime for intercepting communications, data retention and other matters. As I said earlier—and I introduced the Regulation of Investigatory Powers Bill on this basis—its purpose was to make the intrusive powers of the state compatible with the Human Rights Act 1998, which came into force more than two year later on 2 October 2000. I am proud of the 1998 Act and—to reassure and provide therapy to the hon. Member for Cambridge—of the fact that it was indeed a liberal measure, but I of course accept that the world of telecommunications has changed radically in the 14 years since. Interestingly, it has not changed as much as it had changed in the preceding 15 years, which followed the Interception of Communications Act 1985, but it has still

[8] http://www.publications.parliament.uk/pa/cm201415/cmhansrd/cm140715/debtext/140715-0003.htm#14071561000001

	changed a great deal and for sure it would be worth while for RIPA to be reviewed. However, that is not a case for not proceeding with this measure tonight.

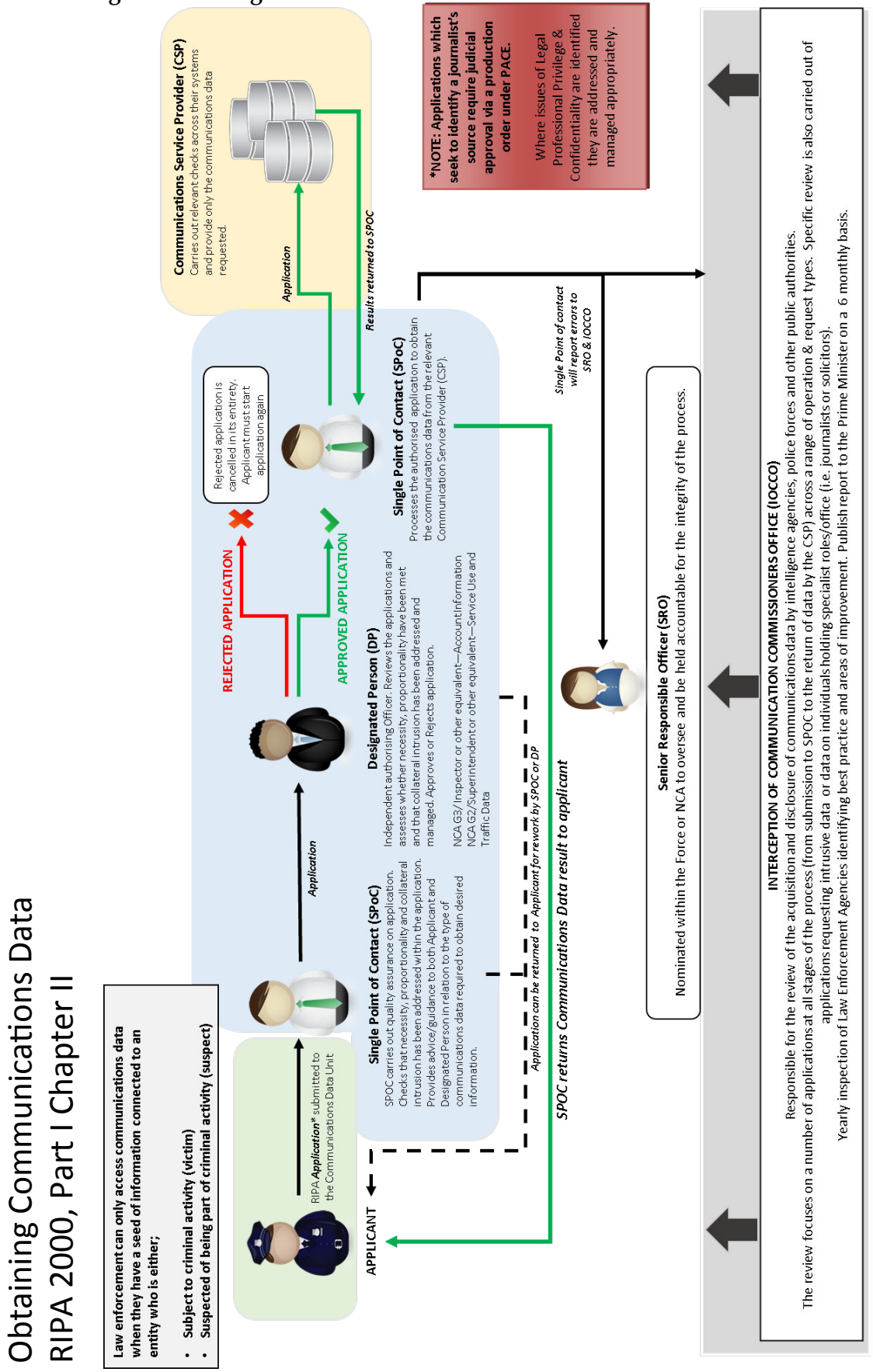
Lords Second Reading: 16 July 2014[9]

The Parliamentary Under-Secretary of State, Home Office (Lord Taylor of Holbeach)	… Communications data—the who, where, when and how of a communication, but not its content—can be used to piece together the activities of suspects, victims and vulnerable people. They can prove or disprove alibis, identify links between potential criminals, tie suspects and victims to a crime scene, and help find vulnerable persons at risk of imminent harm. … Those data are held by communications service providers for their business purposes and where they are required to do so by law. **They are then accessed by law enforcement, subject to stringent safeguards, where it is necessary and proportionate to do so for a specific investigation.**
Lord Armstrong	… I am sure that it is important—indeed **necessary—that there be no doubt about the legality of requirements placed on communications service providers to make communications data other than the content of communications available**, mainly for the detection and prevention of serious crime and of terrorist outrages, but also for other purposes, particularly child protection, and to retain those data for longer than they would need for their own commercial purposes. Yesterday, the Minister described the Bill as a puncture repair to keep the car on the road, not a new tyre. I accept that the Bill does no more than restore the legal cover to the state in which it was, or was believed to be, before the European court's judgment, and as such I believe that noble Lords can and should approve it …
Baroness Kennedy	… It is my concern that the Bill is seeking to provide a lawful basis for the unlawful exercise of power by the UK security agencies. I say that because the Snowden disclosures showed that in fact there was a sharing of information by GCHQ with the American security services. **They were looking into metadata in ways that none of us knew about and which were certainly not covered by RIPA. It meant that the security services were involved in activities that were not covered by law.** It is right that there should be new legislation but this is not the way to do it. It is deeply regrettable that we are having a bite at it in this way.
Lord Strasburger	… But the biggest problem with RIPA is that it contains a deliberate and well concealed loophole that is used to claim legal cover for Project Tempora's hoovering up of everything that everyone does on the internet and storing it. The British people were never asked, via their representatives in Parliament, "How do you feel about the Government helping themselves to all your private data?". **I presume that they were not asked because the Home Office knew what the answer would be—and it would not have been, "Yes please"**, especially if it had been explained that it is as if there is a man or woman from the Ministry looking over your shoulder and making notes whenever you use the internet, at home or at work or on a train, or wherever you are. So instead of getting the permission of the British people, **the Home Office used legislative sleight of hand to slip it in**

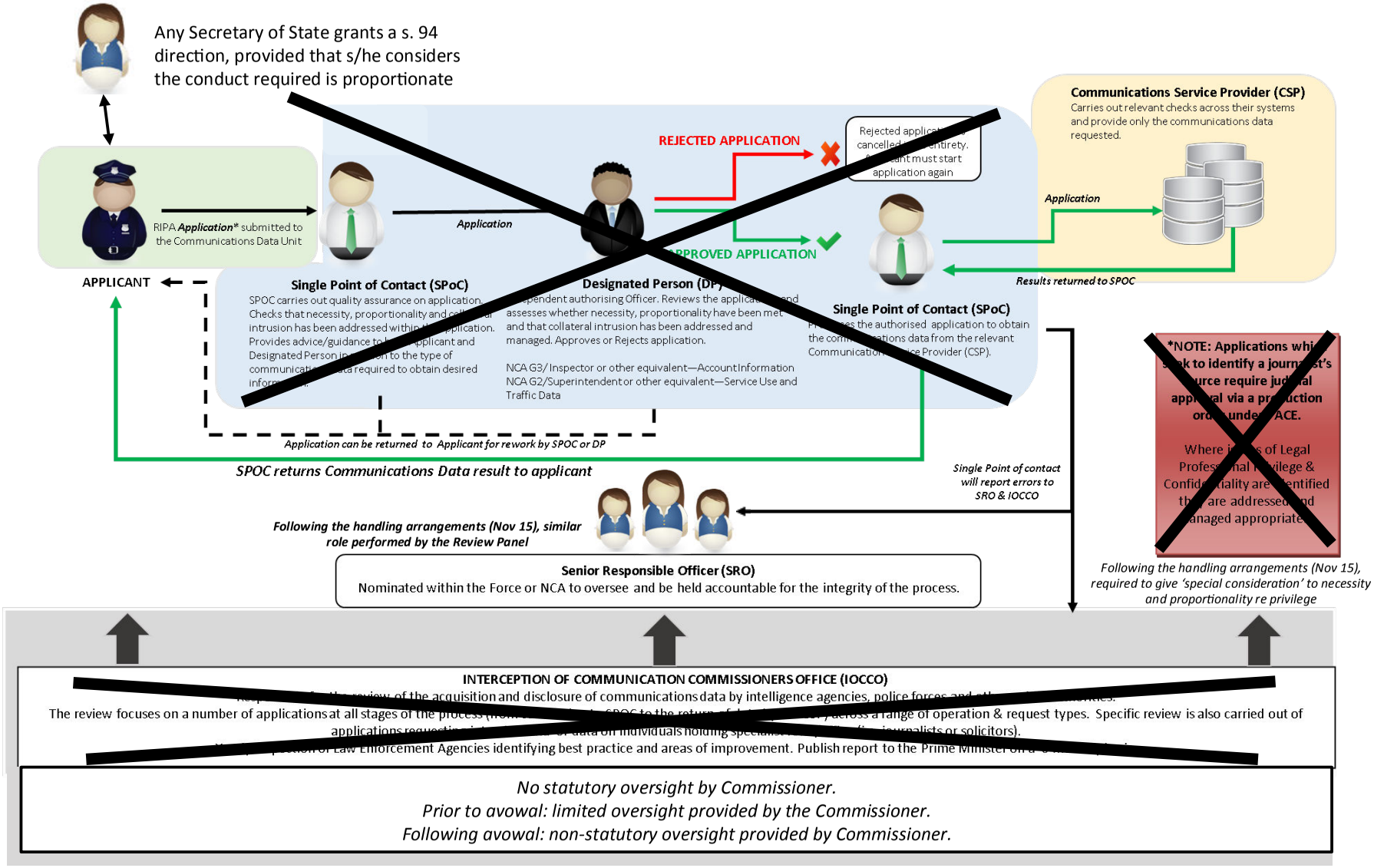
[9] http://www.publications.parliament.uk/pa/ld201415/ldhansrd/text/140716-0001.htm#14071671000140

	under the radar. That must ring alarm bells about related legislation such as this Bill being rushed through without proper scrutiny.
Lord Taylor	In the absence of a clear legal basis for retaining communications data, the police stand to lose access to vital information, which—as has been pointed out—contributes to 95% of serious crime prosecutions. Unless we make clear the obligations that RIPA imposes on companies based overseas but providing services here in the UK, the security and intelligence agencies stand to lose their ability to monitor terrorists and organised crime groups in this country. Indeed, as a number of noble Lords have said, and have agreed with the Government, the Bill does not provide new powers. It does not alter or extend existing powers. It simply provides **a clear legal basis for powers that the police and intelligence agencies have always relied on** to keep people safe, which for different reasons—and there are different reasons within the two parts of the Bill—are now in question. … The noble Lord, Lord Armstrong of Ilminster, asked whether David Anderson's review would cover **all use of communications data**. Clause 7 makes clear that the review covers the operation and regulation of investigatory powers. **That extends to communications data for all purposes under RIPA for which it can be obtained. I hope that that reassures the noble Lord.**

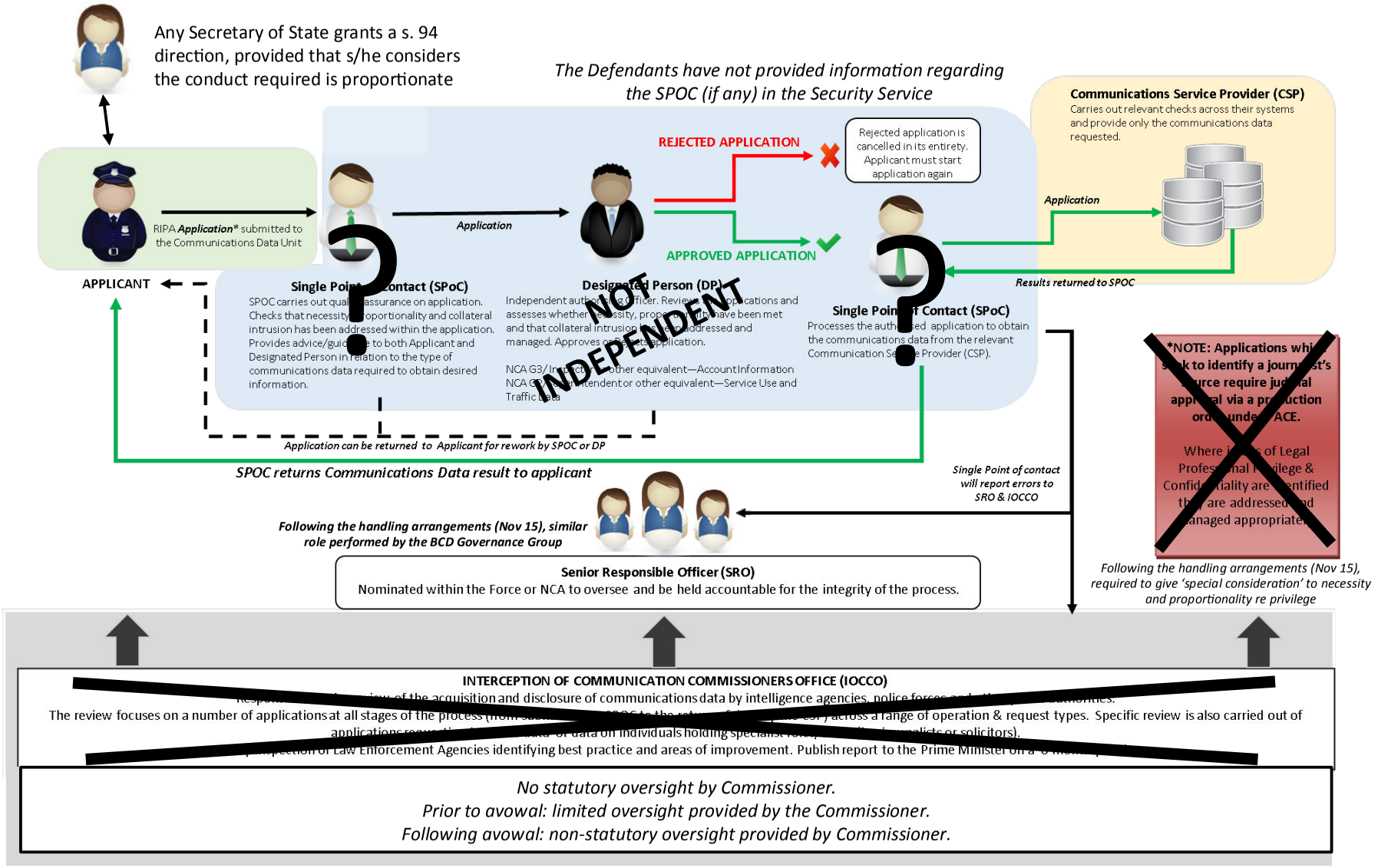
Appendix 2 – Diagrams of Safeguards



Obtaining Communications Data
Section 94 TA, GCHQ



Obtaining Communications Data
Section 94 TA, Security Service



Appendix 3 – IOCCO's Analysis

Sir Stanley Burnton's list of specific requirements (Burnton Report, §§ 4.14-15)	**Reference in the Open Handling Arrangements (4 November 2015)**
What should be in an application to a Secretary of State for a section 94 direction, including guidance in relation to necessity and proportionality	§ 4.1
The duration for which a section 94 direction can be given	-
Procedures specifying how a direction is to be reviewed, renewed, modified or cancelled (and by whom)	§ 4.5
Where a direction relates to the acquisition of BCD the processes and considerations concerning the retention and destruction of data	§ 4.3.2 (requirement to apply protective security measures) § 4.5.3 (requirement to destroy data)
Where a direction relates to the acquisition of BCD, the processes and considerations as to when, how, for what purpose and by whom the data retained may be accessed by a member of a public authority	§ 4.3.3
Matters relating to what constitutes an 'error' in the giving of a direction, any conduct undertaken to comply with the direction, or in the subsequent access to data obtained under a direction, and the process for the reporting of errors	§ 4.6
Requirement for a section 94 direction to be given in writing or in a manner that produces a record of it having been given	-
Requirement for the direction to describe the specific conduct to be undertaken by the PECN	-
Requirement to specify the statutory necessity purpose for which it was given	-
Requirement to specify the name of the Secretary of State giving it and the date it is given and will expire	-
Requirement to specify the manner in which any disclosure is to be made or any conduct required is to be undertaken by the PECN	§ 4.4

Appendix 4 – Claimant's Schedule cross-referenced to main skeleton

Paragraph 6 of the Order of the Tribunal dated 7 July 2016 required the Claimant *'to append to its skeleton argument a table summarising its position in relation to "Access", "Use", "Disclosure", "Retention Period", "Review", "Destruction[*"*] and "Oversight" by reference to the periods in issues 2-4 in the List of Issues appended hereto'.*

The Claimant has sought to summarise its case below, but it is not possible to fully incorporate all the detail in the Re-Amended Grounds and Skeleton in a short table. ~~A version cross-referenced with the Skeleton will be supplied with any Reply Skeleton on Monday.~~ This is the cross-referenced version of the Appendix to the Claimant's main skeleton argument; references in the form **[§§]** are to paragraphs in that document.

The Claimant also notes that in *Szabo & Vissy v Hungary* (Application 37128/14, 12 January 2016) the ECtHR indicated that "*[t]he guarantees required by the extant Convention case-law on interception need to be enhanced*" in view of the impact of "*cutting-edge technologies*" on the scale and effect of such interception. It is no longer sufficient only to examine the six categories *Weber*. The Tribunal should consider what additional safeguards are required to provide protection against arbitrary conduct in the context of modern surveillance techniques.

Section 94 Regime

<table>
<tr><th></th><th>Prior to avowal and the publication of handling arrangements on 4 November 2015</th><th>From 4 November 2015 to date of the hearing</th><th>As at the date of the hearing</th></tr>
<tr><td rowspan="4">Access</td><td colspan="3">Not in accordance with domestic law. [§§ 54-67]</td></tr>
<tr><td colspan="3">No requirement for judicial or independent authorisation, including for journalistic or LPP material. [§ 68g, i]</td></tr>
<tr><td colspan="3">Neither necessary nor proportionate to access BCD under section 94 TA, where there is another, less intrusive means available, nor where there is no judicial or independent authorisation.</td></tr>
<tr><td>Regime entirely secret and therefore insufficiently foreseeable. [§ 68a-b]</td><td colspan="2">Handling arrangements misleading. [§ 72]
GCHQ do not operate any of the safeguards of a RIPA Part I Chapter II process. There is no SPoC or Designated Person. Officers are able to have direct access to data without approval from a senior officer. [§ 73b]
The Security Service do not properly comply with the Communications Data Code of Practice. No evidence of complying with para 3.11 (necessity); no implementation of provisions requiring that the Designated Person be independent of the investigation. [§ 73d]
Fact of non-compliance with the Code kept secret until recently. [§ 73d(v)]</td></tr>
</table>

		Until January 2015, Designated Persons did not have to give any reasons for their decisions. Since January 2015, reasons need only be given in cases involving sensitive professions. **[§ 73d(vi)-(vii)]**	Recommendations in the July 2016 Burnton Report have not been implemented. **[§ 73a]**
Use	Data that can only lawfully be obtained for one purpose (national security) may be re-used for another purpose (e.g. serious crime) **[§ 73g]**		
	Neither necessary nor proportionate to use BCD under section 94 TA, where there is another, less intrusive means available, nor where there is no judicial or independent authorisation for its access. **[§ 83]**		
	No procedures in place to protect privileged material, or to prevent the use of section 94 TA data from being used to uncover a journalistic source. **[§ 68g]**		
	Regime entirely secret and therefore insufficiently foreseeable. **[§ 68a-b]**		
Disclosure	Entire databases of BCD can be shared with foreign partners. GCHQ disclose entire databases of "*raw sigint data*" to industry partners who have been "*contracted to develop new systems and capabilities for GCHQ*". **[§ 73f]** Disclosure may also be made to other government departments (e.g. HMRC). **[§ 73g]**		
	Regime entirely secret and therefore insufficiently foreseeable. **[§ 68a-b]**		
Retention Period	Regime entirely secret and therefore insufficiently foreseeable. **[§ 68a-b]**	BCD is retained for up to one year (MI5 Amended Witness Statement, § 130).	
Review	No statutory provision for the review of s. 94 directions. **[§ 68c]**		
	Regime entirely secret and therefore insufficiently foreseeable. **[§ 68a-b]**		
Destruction	Regime entirely secret and therefore insufficiently foreseeable. **[§ 68a-b]**	(See 'Retention Period').	
Oversight	No statutory oversight. **[§ 68c]**		
	No procedure to notify victims of any misuse of BCD. **[§ 68j]**		
	Regime entirely secret and therefore insufficiently foreseeable. **[§ 68a-b]**	Only from December 2015 were IOCCO able to carry out an audit of	

		the use of s. 94 data. **[§ 68h(v)]**	
	Oversight was not provided on express, agreed terms. From 2004 to 2006, Sir Swinton Thomas provided non-statutory oversight over section 94 directions. Only from February 2015 was oversight extended to cover the necessity and proportionality of section 94 directions. Could not be exercised from this date, however, given that the IOCCO required extra staff and technical facilities. Quality of oversight was inadequate. **[§ 68h]**		

BPD Regime

<table>
<tr><th></th><th>Prior to avowal of BPDs on 12 March 2015</th><th>From 12 March 2015 until the publication of handling arrangements on 4 November 2015</th><th>From 5 November 2015 to the date of the hearing</th><th>As at the date of the hearing</th></tr>
<tr><td rowspan="3">Access</td><td colspan="4">No Secretary of State warrant or independent authorisation is required to obtain BPD. Contrast IP Bill. [§ 82]</td></tr>
<tr><td>Regime entirely secret and therefore insufficiently foreseeable [§ 74]</td><td>No arrangements were made public. The scheme was not sufficiently foreseeable. [§ 81]</td><td colspan="2">Current regime is not sufficiently accessible to the public, nor does it contain adequate safeguards to provide proper protection against arbitrary conduct. [§ 82]</td></tr>
<tr><td>At GCHQ (and possibly the other Agencies), unless the database contained “real names” (defined as “at least the actual names of individuals”), the dataset would not be treated as a BPD or be subject to approval procedures. [§ 78a]
At MI5, all commercially available datasets were excluded from the policy until late 2012 – such that there was no authorisation procedure. Any BPD obtained under RIPA or ISA was excluded from the policy until Autumn 2013. [§ 78b-c]</td><td colspan="3"></td></tr>
<tr><td>Use</td><td>Regime entirely secret and therefore insufficiently foreseeable [§ 74]</td><td>No arrangements were made public. The scheme was not sufficiently foreseeable. [§ 81]

MI5 officials were instructed that the level of intrusion arising from the</td><td colspan="2">Current regime is not sufficiently accessible to the public, nor does it contain adequate safeguards to provide proper protection against arbitrary conduct. [§ 82]</td></tr>
</table>

		holding of data is generally assessed to be very limited. **[§ 78d]**	
	SIS had no requirement to enter the reason for a search before accessing the database. **[§ 78e]**		
Disclosure	No bar on the transfer of entire BPDs to other intelligence agencies outside the UK, even where the recipient will not provide adequate protection or safeguards for the security or use of the dataset. **[§ 82c]**		
	Regime entirely secret and therefore insufficiently foreseeable **[§ 74]**	No arrangements were made public. The scheme was not sufficiently foreseeable. **[§ 81]**	Current regime is not sufficiently accessible to the public, nor does it contain adequate safeguards to provide proper protection against arbitrary conduct. **[§ 82]**
Retention Period	No temporal limits on the retention of data. **[§ 82b]**		
	Regime entirely secret and therefore insufficiently foreseeable. **[§ 74]**	No arrangements were made public. The scheme was not sufficiently foreseeable. **[§ 81]**	
Review	Regime entirely secret and therefore insufficiently foreseeable **[§ 74]** The SIS carried out its first Dataset Retention Review in June 2008 (SIS Witness Statement, § 34). As at 2010, some auditing was carried out, but did not systematically audit access to all non-targeted personal datasets. As at May 2014, GCHQ had not commenced auditing its main corporate BPD tool. At GCHQ (and possibly the other Agencies), unless the database contained "real names" (defined as "at least the actual names of	No arrangements were made public. The scheme was not sufficiently foreseeable. **[§ 81]** In May 2015, GCHQ suspended acquisition of financial datasets until the auditing difficulties were resolved. The current position is unclear.	The Claimant will make submissions on the oversight position after publication of Sir Mark Waller's report. **[§ 84]**

	individuals"), the dataset would not be treated as a BPD or be subject to review and approval procedures.			
Destruction	Regime entirely secret and therefore insufficiently foreseeable **[§ 74]**	No arrangements were made public. The scheme was not sufficiently foreseeable. **[§ 81]**	(See 'Retention Period').	
Oversight	No procedure to notify victims of any misuse of a BPD so that they can seek an appropriate remedy before the Tribunal **[§82d]**			
	Regime entirely secret and therefore insufficiently foreseeable **[§ 74]**	Oversight was placed onto a statutory footing by virtue of the BPD Direction. However, no arrangements were made public. The scheme was not sufficiently foreseeable. **[§ 81]**	Arrangements were not made public until their disclosure in this case. **[§ 81]**	
	No statutory oversight. Oversight by the Commissioners began at the end of 2010 and was inadequate. **[§§ 79-80]** - December 2011: Sir Paul Kennedy examined the authorisation forms for a single dataset. - Sir Mark Waller has not audited the use of any BPD, nor considered the increase in privacy interference when multiple datasets are used to create profiles.			

Case No. IPT/15/110/CH

IN THE INVESTIGATORY POWERS TRIBUNAL

B E T W E E N:

PRIVACY INTERNATIONAL

Claimant

-and-

(1) SECRETARY OF STATE FOR FOREIGN AND COMMONWEALTH AFFAIRS
(2) SECRETARY OF STATE FOR THE HOME DEPARTMENT
(3) GOVERNMENT COMMUNICATIONS HEADQUARTERS
(4) SECURITY SERVICE
(5) SECRET INTELLIGENCE SERVICE

Respondents

CLAIMANT'S SKELETON ARGUMENT IN REPLY

For hearing commencing: Tuesday 26 July 2016

Privacy International
62 Britton Street
London
EC1M 5UY

Bhatt Murphy
27 Hoxton Square, London N1 6NN
DX: 36626 Finsbury