Respondents' Response to the Claimant's Appendix

In an Appendix to its skeleton argument, the Claimant summarised its position in relation to *"Access"*, *"Use"*, *"Disclosure"*, *"Retention Period"*, *"Review"*, *"Destruction["] and "Oversight"* by reference to the periods in issues 2-4 as required by paragraph 6 of the Order of 7 July 2016.

The Claimant's table is reproduced below. The Respondents set out their responses to the Claimant's position in bold. The responses below are only intended as a summary of the Respondents' position, which is set out more fully in the Respondents' skeleton argument.

Section 94 Regime

	Prior to avowal and the publication of handling arrangements on 4 November 2015	**From 4 November 2015 to date of the hearing**	**As at the date of the hearing**
Access	Not in accordance with domestic law. **Not accepted: see Respondent's skeleton argument, §§8-60.**		
	No requirement for judicial or independent authorisation, including for journalistic or LPP material. **Prior judicial or independent authorisation is not a requirement of Article 8 ECHR.**		
	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. **The Section 94 Regime was and is proportionate for the reasons given at §§173-177 of the Respondents' skeleton argument.** **Prior judicial or independent authorisation is not a requirement of Article 8 ECHR.**		

	Regime entirely secret and therefore insufficiently foreseeable. **Not accepted: see Respondents' skeleton argument, at §66(a) and the statutory safeguards and the safeguards applied as a matter of practice and policy in the Acquisition and Disclosure of Communications Data/Interception of Communications Codes of Practice, as set out in Appendix A to the Respondents' skeleton.**	Handling arrangements misleading. **The Respondents do not accept that the Section 94 Handling Arrangements were misleading. They set out Handling Arrangements to be applied at GCHQ and MI5 in respect of Bulk Communications Data obtained under section 94, irrespective of the underlying procedures used by those agencies. The matters set out at §72 of the Claimant's skeleton argument were either not required to be stated in the Section 94 Handling Arrangements, or in the case of §72(c) were accurately stated in the Section 94 Handling Arrangements.** 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. **The safeguards applied by GCHQ were adequate, as set out at §§98-103 of the Respondents' skeleton argument.** 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. Fact of non-compliance with the Code kept secret until recently. **It is not accepted that the matters relied on meant that the Section 94 Regime at MI5 was not in accordance with law. Further, the allegation in respect of compliance with para. 3.11 is unclear and unparticularised in the Appendix and not further or adequately explained in the Claimant's skeleton argument.**	
		Until January 2015, Designated Persons did not have to give any reasons for their decisions. Since	Recommendations in the July 2016 Burnton Report have not been implemented.

		January 2015, reasons need only be given in cases involving sensitive professions. **It is not accepted that the matters relied on meant that the Section 94 Regime at MI5 was not in accordance with law.**	**The July 2016 Burnton Report [Auths/tab 82] expressly (at §3.3) did not state a view on whether or not the Section 94 Regime was in accordance with law under Article 8(2) ECHR. For the avoidance of doubt, it is denied that the matters set out in his report render the Section 94 Regime not "in accordance with law". It is, and was, in accordance with law for the reasons set out at §§75-123 of the Respondents' skeleton, the extensive safeguards (set out at Appendix A to the skeleton) in place for Section 94.**
Use	Data that can only lawfully be obtained for one purpose (national security) may be re-used for another purpose (e.g. serious crime) **The practice referred to is lawful: see section 19(2) of the Counter-Terrorism Act 2008 (Appendix A to the Respondents' skeleton, §14)**		
	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. **The Section 94 Regime was and is proportionate for the reasons given at §§173-177 of the Respondents' skeleton argument.** **Prior judicial or independent authorisation is not a requirement of Article 8 ECHR.**		
	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. **Not accepted. GCHQ applied safeguards in respect of privileged material and confidential journalistic material: see pp.117-122 and pp.9-12 of the GCHQ exhibit. MI5 applied safeguards in the Acquisition and Disclosure of Communications Data Codes of Practice, and the guidance at pp. 143-152 of the MI5 exhibit, and specifically that at p.149 (foot of page) and 150 (first paragraph).**	
	Regime entirely secret and therefore insufficiently foreseeable. **Not accepted: see Respondents' skeleton argument, at §66(a) and the statutory safeguards and the safeguards applied as a matter of practice and policy in the Acquisition and Disclosure of Communications Data/Interception of Communications Codes of Practice, as set out in Appendix A to the Respondents' skeleton.**	
Disclosure	Entire databases of BCD can be shared with foreign partners. **Disclosure of BCD was, and remains, subject to safeguards, as set out at §§86-89, 100(c), 103, 117, 121-122 of the Respondents' skeleton argument. It is not accepted that the Section 94 Regime was unlawful because it was possible, provided that those safeguards were met, to share BCD 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*". **Disclosure of "sigint data" to industry partners, for the specific purpose of assisting them to development new systems and capabilities to GCHQ was permitted, subject to safeguards: see Bundle 3, pp. 476-482. Those safeguards included the requirement of proportionality, i.e. "whether the requirement could be fulfilled with less data." (*ibid.*, p.476). It is denied that this limited purpose, accompanied with appropriate safeguards, rendered the s.94 Regime not "in accordance with law."** Disclosure may also be made to other government departments (e.g. HMRC). **It is not accepted that this is unlawful: see §§53-60 of the Respondents' skeleton argument.**	
	Regime entirely secret and therefore insufficiently foreseeable. **Not accepted: see Respondents' skeleton argument, at §66(a) and the statutory safeguards and the safeguards applied as a matter of practice and policy in the Acquisition and Disclosure of Communications Data/Interception of Communications Codes of Practice, as set out in Appendix A to the Respondents' skeleton.**	
Retention Period	Regime entirely secret and therefore insufficiently foreseeable. **Not accepted: see Respondents' skeleton argument, at §66(a) and the statutory safeguards and the safeguards applied as a**	BCD is retained for up to one year (MI5 Amended Witness Statement, § 130). **It is denied that the retention period referred to is not in accordance with law. The Respondents reserve the right to respond further to this assertion if reasons are given for it (no reasons having been given in**

	matter of practice and policy in the Acquisition and Disclosure of Communications Data/Interception of Communications Codes of Practice, as set out in Appendix A to the Respondents' skeleton.	**the Claimant's skeleton or Appendix).**
Review	No statutory provision for the review of s. 94 directions. **It is not accepted that a statutory provision for such a review is required in order for the Section 94 Regime to be "in accordance with law".**	
	Regime entirely secret and therefore insufficiently foreseeable. **Not accepted: see Respondents' skeleton argument, at §66(a) and the statutory safeguards and the safeguards applied as a matter of practice and policy in the Acquisition and Disclosure of Communications Data/Interception of Communications Codes of Practice, as set out in Appendix A to the Respondents' skeleton.**	
Destruction	Regime entirely secret and therefore insufficiently foreseeable. **Not accepted: see Respondents' skeleton argument, at §66(a) and the statutory safeguards and the safeguards applied as a matter of practice and policy in the Acquisition and Disclosure of**	(See 'Retention Period'). **See response under 'Retention Period' above.**

	Communications Data/Interception of Communications Codes of Practice, as set out in Appendix A to the Respondents' skeleton.		
Oversight	No statutory oversight. **It is not accepted that statutory oversight is or was required for the Section 94 Regime to be in accordance with law. The oversight which existed and exists over Section 94 BCD was at all times adequate: see §§92-97 and 118-120 of the Respondents' skeleton argument.**		
	No procedure to notify victims of any misuse of BCD. **It is denied that the absence of such a mechanism means that the BCD regime is not in accordance with law under Art 8(2). There is no such requirement in ECtHR case law. In any event, the Respondents' internal audit procedures and the oversight of the Interception of Communications Commissioner and of the Intelligence and Security Committee are sufficient safeguards against misuse such as to render the BCD Regime in accordance with law.**		
	Regime entirely secret and therefore insufficiently foreseeable. **Not accepted: see Respondents' skeleton argument, at §66(a) and the statutory safeguards and the safeguards applied as a matter of practice and policy in the Acquisition and Disclosure of Communications Data/Interception of Communications Codes of Practice, as set out in Appendix A to the Respondents' skeleton.**	Only from December 2015 were IOCCO able to carry out an audit of the use of s. 94 data. **If this is intended to allege that there was no audit of the use of s.94 data before December 2015, that is not accepted.** **Use of GCHQ's s.94 data was audited by the Interception of Communications Commissioner in this period: see response to request 81 of the Amended Response to the Claimant's Supplementary Request for Further Information and**	

		Disclosure [Core/tab 9]. **As for MI5, it is denied (if it is intended to be asserted) that there was any inadequacy in the oversight of s.94 data: see the response to request 88 in the Amended Response to the Claimant's Supplementary Request for Further Information [Core/tab 9.]**	
	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. **It is not accepted that the oversight regime was inadequate: see §§92-97 and 118-120 of the Respondents' skeleton argument.**		

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>Access</td><td colspan="4">No Secretary of State warrant or independent authorisation is required to obtain BPD. Contrast IP Bill.

Warrants/authorisations required where BPDs obtained by RIPA/ISA powers. Insofar as BPDs are not obtained by RIPA/ISA powers, the absence of a warrant/independent authorisation requirement does not render the BPD Regime not in accordance with law:
(i) Acquisition of BPDs is subject to the statutory safeguards set out in Appendix B to the Respondents' skeleton, as well as the safeguards set out at §§135-144 to that Appendix;
(ii) Acquisition must be approved by a senior official with the acquiring agency, and may be the subject of a submissions to a Secretary of State or Minister;
(iii) Acquisition is subject to oversight by the Intelligence Services Commissioner.

In the circumstances, it is not accepted that the absence of a warrant/authorisation in cases where BPDs are not obtained by RIPA/ISA renders or rendered the BPD Regime not in accordance with law.</td></tr>
<tr><td></td><td>Regime entirely secret and therefore insufficiently foreseeable

Not accepted: see Respondents' skeleton argument, at §66(b) and the statutory safeguards, together with the safeguards set out in the relevant Codes of Practice in the case of acquisition under RIPA/ISA, as set out in Appendix B to the Respondents' skeleton.</td><td>No arrangements were made public. The scheme was not sufficiently foreseeable.

Not accepted: see Respondents' skeleton argument, at §66(b) and the statutory safeguards, together with the</td><td>Current regime is not sufficiently accessible to the public, nor does it contain adequate safeguards to provide proper protection against arbitrary conduct.

The assertion that the current BPD regime is "not sufficiently accessible to the public" is not particularised in the Appendix, but appears (from the Claimant's skeleton, §82(d)) to be premised on the lack of a mechanism for those affected by use of BPDs to be informed,</td><td></td></tr>
</table>

		safeguards set out in the relevant Codes of Practice in the case of acquisition under RIPA/ISA, as set out in Appendix B to the Respondents' skeleton. **Further, the BPD Regime became more transparent after the publication of the ISC's *Privacy and Security* report.**	**and to be able to bring a complaint to the Tribunal.** **It is denied that the absence of such a mechanism means that the BPD regime is not in accordance with law under Art 8(2). There is no such requirement in ECtHR case law. In any event, the Respondents' internal audit procedures and the oversight of the Intelligence Services Commissioner and of the Intelligence and Security Committee are sufficient safeguards against misuse such as to render the BPD Regime in accordance with law.**
	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. **This policy, which ceased in February 2015 with the coming into force of the SIA Joint BPD Policy, did not in any event prevent the BPD Regime being in accordance with law.** At MI5, all commercially available datasets were excluded from the policy until late 2012 – such that there was no authorisation procedure. **In fact, as noted in the MI5 witness statement, §70, MI5 excluded "all commercially *and openly***	**The Respondents note that no criticisms in respect of "access" appear to be made for these periods. The criticisms made of the period before March 2015 all relate to policies which were amended before March 2015.**	

	available" (emphasis added) datasets from the BPD regime. Examples include data from Companies House. It is denied that the omission to include such openly available datasets within the BPD Regime meant that it was not in accordance with law up to late 2012. Any BPD obtained under RIPA or ISA was excluded from the policy until Autumn 2013. **It is denied that this meant that the BPD Regime was not in accordance with law. BPDs obtained under RIPA or ISA were subject to the relevant Codes of Practice, which provided adequate safeguards.**		
Use	Regime entirely secret and therefore insufficiently foreseeable **Not accepted: see Respondents' skeleton argument, at §66(b) and the statutory safeguards, together with the safeguards set out in the relevant Codes of Practice in the case of acquisition under RIPA/ISA, as set out in Appendix B to the Respondents' skeleton.**	No arrangements were made public. The scheme was not sufficiently foreseeable. **Not accepted: see Respondents' skeleton argument, at §66(b) and the statutory safeguards, together with the safeguards set out in the relevant Codes of Practice in the case of acquisition under RIPA/ISA, as set out**	Current regime is not sufficiently accessible to the public, nor does it contain adequate safeguards to provide proper protection against arbitrary conduct. **The assertion that the current BPD regime is "not sufficiently accessible to the public" is not particularised in the Appendix, but appears (from the Claimant's skeleton, §82(d)) to be premised on the lack of a mechanism for those affected by use of BPDs to be informed, and to be able to bring a complaint to the Tribunal.** **It is denied that the absence of such a mechanism means that the BPD regime is not**

		in Appendix B to the Respondents' skeleton. **Further, the BPD Regime became more transparent after the publication of the ISC's *Privacy and Security* report.** MI5 officials were instructed that the level of intrusion arising from the holding of data is generally assessed to be very limited. **It is denied that the BPD Regime was unlawful under Article 8(2) ECHR because of the reference in the MI5 guidance to the phrase "very limited". That phrase is not inconsistent with the ECtHR authorities cited by the Claimant, and in any event must be read in the context**	**in accordance with law under Art 8(2). There is no such requirement in ECtHR case law. In any event, the Respondents' internal audit procedures and the oversight of the Intelligence Services Commissioner and of the Intelligence and Security Committee are sufficient safeguards against misuse such as to render the BPD Regime in accordance with law.**

		of the guidance more generally, which provided more detailed guidance on the degree of intrusion than the Claimant's selected quotation suggests, and also required legal adviser approval of the assessment of intrusion.	
	SIS had no requirement to enter the reason for a search before accessing the database. **It is denied that the absence of such a requirement means the BPD Regime at SIS was not in accordance with law. There were adequate safeguards in place in the form of, inter alia:** **(i) the Code of Practice which all users were required to sign before being given access to the database;** **(ii) Commissioner oversight.**		
	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. **The safeguards in place in respect of disclosure were adequate at all of the relevant periods: see §§134-137, 145, 147, 150, 154, 158-160, 164, 168-170 of the Respondents' skeleton argument. See e.g. §7.3.1 of the SIS BPD Handling Arrangements (3/413); §9.6 of the GCHQ BPD Handling Arrangements (4/A/143) and §6.3.2 of the MI5 BPD Handling Arrangements (1/110);**		

	Regime entirely secret and therefore insufficiently foreseeable **Not accepted: see Respondents' skeleton argument, at §66(b) and the statutory safeguards, together with the safeguards set out in the relevant Codes of Practice in the case of acquisition under RIPA/ISA, as set out in Appendix B to the Respondents' skeleton.**	No arrangements were made public. The scheme was not sufficiently foreseeable. **Not accepted: see Respondents' skeleton argument, at §66(b) and the statutory safeguards, together with the safeguards set out in the relevant Codes of Practice in the case of acquisition under RIPA/ISA, as set out in Appendix B to the Respondents' skeleton.** **Further, the BPD Regime became more transparent after the publication of the ISC's *Privacy and Security* report.**	Current regime is not sufficiently accessible to the public, nor does it contain adequate safeguards to provide proper protection against arbitrary conduct. **The assertion that the current BPD regime is "not sufficiently accessible to the public" is not particularised in the Appendix, but appears (from the Claimant's skeleton, §82(d)) to be premised on the lack of a mechanism for those affected by use of BPDs to be informed, and to be able to bring a complaint to the Tribunal.** **It is denied that the absence of such a mechanism means that the BPD regime is not in accordance with law under Art 8(2). There is no such requirement in ECtHR case law. In any event, the Respondents' internal audit procedures and the oversight of the Intelligence Services Commissioner and of the Intelligence and Security Committee are sufficient safeguards against misuse such as to render the BPD Regime in accordance with law.**
Retention Period	No temporal limits on the retention of data. **It is denied, if it is intended to be asserted, that there are, and have been, no retention periods in respect of BPDs. Further, and in any event, it is not a requirement under Art 8(2) ECHR that specified retention periods be in force, provided that**		

	retention is both necessary and proportionate: see §§82, 94-99, 117-118, 120(d), 149-150, , 158, 160(c) of Appendix B to the Respondents' skeleton argument.		
	Regime entirely secret and therefore insufficiently foreseeable. **Not accepted: see Respondents' skeleton argument, at §66(b) and the statutory safeguards, together with the safeguards set out in the relevant Codes of Practice in the case of acquisition under RIPA/ISA, as set out in Appendix B to the Respondents' skeleton.**	No arrangements were made public. The scheme was not sufficiently foreseeable. **Not accepted: see Respondents' skeleton argument, at §66(b) and the statutory safeguards, together with the safeguards set out in the relevant Codes of Practice in the case of acquisition under RIPA/ISA, as set out in Appendix B to the Respondents' skeleton.** **Further, the BPD Regime became more transparent after the publication of the ISC's *Privacy and Security* report.**	
Review	Regime entirely secret and therefore insufficiently foreseeable	No arrangements were made public. The scheme was not	The Claimant will make submissions on the oversight position after publication of Sir Mark Waller's report.

	The SIS carried out its first Dataset Retention Review in June 2008 (SIS Witness Statement, § 34). **This allegation is unclear (and not repeated or further explained in the Claimant's skeleton) but for the avoidance of doubt it is denied that it meant that the BPD Regime was not in accordance with law.** As at 2010, some auditing was carried out, but did not systematically audit access to all non-targeted personal datasets. **Each of the agencies had auditing procedures in place. Each logged all use of bulk data search tools. GCHQ required users to record their justification for each use. SIS had a comprehensive audit framework in place. MI5 and GCHQ carried out some auditing. See the Hannigan Review [3/571, at §33]. In the circumstances, the procedures for auditing at all of the agencies were in accordance with law under Art 8(2) in this period.** As at May 2014, GCHQ had not commenced auditing its main corporate BPD tool. **This assertion is factually incorrect. GCHQ had commenced auditing its main corporate BPD tool. Specifically, it audited the Necessity and Proportionality justifications provided by those accessing BPDs on the tool. A (if not *the*) key process for access to BPDs was thus audited.**	sufficiently foreseeable. **Not accepted: see Respondents' skeleton argument, at §66(b) and the statutory safeguards, together with the safeguards set out in the relevant Codes of Practice in the case of acquisition under RIPA/ISA, as set out in Appendix B to the Respondents' skeleton.** **Further, the BPD Regime became more transparent after the publication of the ISC's *Privacy and Security* report.** In May 2015, GCHQ suspended acquisition of financial datasets until the auditing difficulties were resolved. The current position is unclear.	**It is unclear why the Claimant requires sight of Sir Mark Waller's report in order to make submissions. However, it appears that the Claimant has no independent criticisms of "Review" in this period.**

	However, GCHQ had not yet commenced an additional, automated, layer of auditing in the form of security "tripwires" which could detect non-compliance with its procedures. It is denied that it was necessary for that additional layer of auditing to have commenced in order for the BPD Regime to be in accordance with law. 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 review and approval procedures. **This policy, which ceased in February 2015 with the coming into force of the SIA Joint BPD Policy, did not in any event prevent the BPD Regime being in accordance with law.**	**It is not accepted that the issue referred to meant that the BPD Regime at GCHQ was not in accordance with law. The issue was as follows: as a result of a high turnover of staff, difficulties arose in assigning the required "Data Sponsor" to a number of financial BPDs. Access to those BPDs was therefore suspended until such time as Data Sponsors could be assigned. The current position is that some of the BPDs in question have since been deleted as a review concluded that they were no longer of sufficient usefulness. In the remainder of cases, Data Sponsors have now been assigned.**	
Destruction	Regime entirely secret and therefore insufficiently	No arrangements	(See 'Retention Period').

	foreseeable **Not accepted: see Respondents' skeleton argument, at §66(b) and the statutory safeguards, together with the safeguards set out in the relevant Codes of Practice in the case of acquisition under RIPA/ISA, as set out in Appendix B to the Respondents' skeleton.**	were made public. The scheme was not sufficiently foreseeable. **Not accepted: see Respondents' skeleton argument, at §66(b) and the statutory safeguards, together with the safeguards set out in the relevant Codes of Practice in the case of acquisition under RIPA/ISA, as set out in Appendix B to the Respondents' skeleton.** **Further, the BPD Regime became more transparent after the publication of the ISC's *Privacy and Security* report.**	**See above in respect of '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. **It is denied that the absence of such a mechanism means that the BPD regime is not in accordance with law under Art 8(2). There is no such requirement in ECtHR case law. In any event, the Respondents' internal audit procedures and the oversight of the Intelligence Services Commissioner and of the Intelligence and Security Committee are sufficient safeguards against misuse such as to render the BPD Regime in accordance with law.**		

	Regime entirely secret and therefore insufficiently foreseeable **Not accepted: see Respondents' skeleton argument, at §66(b) and the statutory safeguards, together with the safeguards set out in the relevant Codes of Practice in the case of acquisition under RIPA/ISA, as set out in Appendix B to the Respondents' skeleton.**	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. **Not accepted: see Respondents' skeleton argument, at §66(b) and the statutory safeguards, together with the safeguards set out in the relevant Codes of Practice in the case of acquisition under RIPA/ISA, as set out in Appendix B to the Respondents' skeleton.** **Further, the BPD Regime became more transparent after the publication of the ISC's *Privacy and Security* report. In**	Arrangements were not made public until their disclosure in this case. **This is not accepted. The BPD Handling Arrangements, which were published in November 2015, gave sufficient detail as to the nature of the oversight regime.**	
	No statutory oversight. Oversight by the Commissioners began at the end of 2010 and was inadequate. - 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. **The Respondents do not accept that the Commissioners' non-statutory oversight was inadequate. The Tribunal is invited to consider the totality of the evidence on this topic: see §§140-143, 145, 147 ("Oversight"), 156 and 166.**			

		addition, the oversight aspect of the BPD Regime was sufficiently foreseeable given the terms of the Intelligence Services Commissioner (Additional Review Functions) Bulk Personal Datasets) Direction 2015 [**Auths/tab 16**]		