IN THE EUROPEAN COURT OF HUMAN RIGHTS **App. No. 58170/13**

BETWEEN:

(1) BIG BROTHER WATCH;
(2) OPEN RIGHTS GROUP;
(3) ENGLISH PEN; AND
(4) DR CONSTANZE KURZ

Applicants

- v -

UNITED KINGDOM

Respondent

UPDATE SUBMISSIONS OF THE APPLICANTS

These submissions are accompanied by a timeline of relevant developments since the Application, which links to the documents referred to for the Court's ease of use. Where documents are referred to below, please refer to the timeline unless otherwise noted.

References in the format [AB/] are to page numbers in the Application Bundle. References to [Annex **] are to the annexes to these submissions. Other references [§**]/(p.**) are to internal numbering within the referenced document.**

PART I: INTRODUCTION

1. This Application was lodged on 29 September 2013. On 9 January 2014, it was communicated to the United Kingdom Government on both admissibility and merits **[Statement of Facts 9-1-14]**.

2. On 8 April 2014, the Application was stayed pending domestic proceedings in the Investigatory Powers Tribunal ("**IPT**") which raised a number of similar issues **[Court Letter 11-4-14]**.

3. The IPT has now handed down two judgments in *Liberty & others v The Government Communications Headquarters & Others*, the first on 5 December 2014 addressing complaints relating to the UK's interception regime (the "TEMPORA issue") and the use by UK intelligence services of US intercept data (the "PRISM issue") **[UK Letter 5-12-14]**. On 6 February 2015, the IPT delivered a second judgment addressing the PRISM issue and concluding that there had been a breach of Article 8 prior to disclosures that had been made by the Government in the course of the proceedings **[UK Letter 15-2-15]**. There is no appeal by either side from judgments of the IPT to a court.

4. It is submitted that the Application should now proceed, and the Government should be required to provide its representations on both admissibility and merits (which the Court has determined it will consider together), and in accordance with the prioritization which the Court has afforded to this important Application.

5. These submissions update the Application in three ways:

   5.1. PART II provides an update in relation to the TEMPORA issue (the UK's own interception) by reference to various developments and the IPT proceedings.

   5.2. PART III provides an update in relation to the PRISM issue (the UK's use of US intercept data).

   5.3. PART IV addresses the issue of exhaustion of remedies.

PART II: TEMPORA ISSUE: UPDATE (APPLICATION PART III. D [§§140-178])

(a) The position of International and European institutions on GCHQ's interception regime

6. Since the Application was filed, a number of international institutions have raised concerns about the UK's interception regime.

7. On 18 December 2013, the UN General Assembly adopted Resolution 68/167 (A/RES/68/167) on the right to privacy in the digital age[1], which stated that the GA:

> "[Was] *Deeply concerned* at the negative impact that surveillance and/or interception of communications, including extraterritorial surveillance and/or interception of communications, as well as the collection of personal data, in particular when carried out on a mass scale, may have on the exercise and enjoyment of human rights,
> *Reaffirming* that States must ensure that any measures taken to combat terrorism are in compliance with their obligations under international law, in particular international human rights, refugee and humanitarian law,"
>
> 1. Reaffirms the right to privacy, according to which no one shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, and the right to the protection of the law against such interference, as set out in article 12 of the Universal Declaration of Human Rights1 and article 17 of the International Covenant on Civil and Political Rights;
>
> 2. Recognizes the global and open nature of the Internet and the rapid advancement in information and communications technologies as a driving force in accelerating progress towards development in its various forms;
>
> 3. Affirms that the same rights that people have offline must also be protected online, including the right to privacy; "

[1] See also Resolution A/C.3/69/L.26/Rev.1 dated 26.11.14.

8. The Resolution called upon States to protect the right to privacy and to review procedures, practices and legislation governing interception of communications to ensure full and effective protection of obligations under international human rights law.

9. Similarly, on 12 March 2014, the EU Parliament adopted a resolution on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs (2013/2188(INI)). The recitals of that resolution recorded that the Parliament had express regard to this Application (*Big Brother Watch & Ors v United Kingdom*). Amongst the Parliament's Main Findings were:

> "compelling evidence of the existence of far-reaching, complex and highly technologically advanced systems designed by US and some Member States' intelligence services to collect, store and analyse communication data, including content data, location data and metadata of all citizens around the world, on an unprecedented scale and in an indiscriminate and non-suspicion-based manner." (Main Findings [§1])

10. The TEMPORA programme was identified as one such programme. It found that "*trust has been profoundly shaken*" (Main Findings [§4]) and stated:

> "5. [….] several governments claim that these mass surveillance programmes are necessary to combat terrorism; [the Parliament] strongly denounces terrorism, but strongly believes that the fight against terrorism can never be a justification for untargeted, secret, or even illegal mass surveillance programmes; takes the view that such programmes are incompatible with the principles of necessity and proportionality in a democratic society.
> […]
> 7. Considers that data collection of such magnitude leaves considerable doubts as to whether these actions are guided only by the fight against terrorism, since it involves the collection of all possible data of all citizens; points, therefore, to the possible existence of other purpose including political and economic espionage, which need to be comprehensively dispelled:
> […]
> 10. Condemns the vast and systemic blanket collection of the personal data of innocent people, often including intimate personal information; emphasises that the systems of indiscriminate mass surveillance by intelligence services constitute a serious interference with the fundamental rights of citizens; stresses that privacy is not a luxury right, but is the foundation stone of a free and democratic society; points out, furthermore, that mass surveillance has potentially severe effects on freedom of the press, thought and speech and on freedom of assembly and of association, as well as entailing a significant potential for abusive use of the information gathered against political adversaries; emphasises that these mass surveillance activities also entail illegal actions by intelligence services and raise questions regarding the extraterritoriality of national laws". (p.11)

11. The Resolution also called, "*on the United Kingdom, in particular, given the extensive media reports referring to mass surveillance by the intelligence service GCHQ, to revise its current legal framework, which is made up of a 'complex interaction' between three separate pieces of legislation – the Human Rights Act 1998, the Intelligence Services Act 1994 and the Regulation of Investigatory Powers Act 2000*" (Recommendations [§24]).

12. On 10 April 2014, an EU Data Protection Working Party, set up under Article 29 of EU Directive 95/46/EC as an independent European advisory body on data

protection and privacy, published its "*Opinion 2014 on surveillance of electronic communications for intelligence and national security purposes*", stating inter alia that:

> "the Working Party concludes that secret, massive and indiscriminate surveillance programs are incompatible with our fundamental laws and cannot be justified by the fight against terrorism or other important threats to national security. Restrictions to the fundamental rights of all citizens could only be accepted if the measure is strictly necessary and proportionate in a democratic society." (p.1)

13. At the request of the UN GA (UN GA Res. 68/167), the Office of the UN High Commissioner for Human Rights ("UNHCHR**"**) reported on these matters in a report published on 30 June 2014 ("*The right to privacy in the digital age*" A/HRC/37). The UNHCHR stated:

> "Where there is a legitimate aim and appropriate safeguards are in place, a State might be allowed to engage in quite intrusive surveillance; however, the onus is on the Government to demonstrate that interference is both necessary and proportionate to the specific risk being addressed. Mass or "bulk" surveillance programmes may thus be deemed to be arbitrary, even if they serve a legitimate aim and have been adopted on the basis of an accessible legal regime. In other words, it will not be enough that the measures are targeted to find certain needles in a haystack; the proper measure is the impact of the measures on the haystack, relative to the harm threatened; namely, whether the measure is necessary and proportionate."(at [§25], p.9).

14. The UN Special Rapporteur on Terrorism shared this view. In his fourth annual report dated 23 September 2014 (A/69/397), he noted that "[t]*he communications of literally every Internet user are potentially open for inspection by intelligence and law enforcement agencies in the States concerned. This amounts to a systematic interference with the right to respect for the privacy of communications, and requires a correspondingly compelling justification"* (at [§9], p.4). The Special Rapporteur concluded that "[t]*he hard truth is that the use of mass surveillance technology effectively does away with the right to privacy of communications on the Internet altogether*" (at [§12], p.5). In short, "*mass surveillance of digital content and communications data presents a serious challenge to an established norm of international law*" (at [§18], p.7).

15. In December 2014, the Council of Europe's Commissioner for Human Rights ("**the CoE Commissioner**") published an Issues paper ("*The rule of law on the internet and in the wider digital world*"), in which he concluded that "[u]*ntil the rules are known under which the agencies and services operate – domestically, extraterritorially or in co-operation with each other – their activities cannot be said to be in accordance with the rule of law. Another matter of serious concern is the manifest ineffectiveness of many supervisory systems*. (p.19)

16. On 26 January 2015, the Committee on Legal Affairs and Human Rights of the Council of Europe adopted a draft resolution for the Parliamentary Assembly. This draft expresses "*deep concern*" about mass surveillance practices. It also states:

> "9. In several countries, a massive "Surveillance-Industrial Complex" has evolved, fostered by the culture of secrecy surrounding surveillance operations, their highly technical character and the fact that both the seriousness of alleged threats and the need for specific counter-measures and their costs and benefits are difficult to assess for political and budgetary decision-makers without relying on input from interested

groups themselves. These powerful structures risk escaping democratic control and accountability and threaten the free and open character of our societies.
10. The Assembly notes that the law in most states provides some protection for the privacy of their own citizens, but not of foreigners. The Snowden files have shown that the NSA and their foreign partners, in particular among the "Five Eyes" partners (United States, United Kingdom, Canada, Australia, New Zealand) circumvent national restrictions by exchanging data on each other's citizens."

17. There has also been concern expressed by the Court of Justice of the European Union ("**CJEU**"). In Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger* (ECLI:EU:C:2014:238) both the Advocate General and the Court considered the indiscriminate retention of data to be a "*particularly serious*" interference which could potentially affect the entire European population's use of communications and consequently its freedom of expression: [§70] of the AG's Opinion (ECLI:EU:C:2013:845) and [§§27-28 and 65] of the CJEU's judgment.

(b) Metadata

18. The Applicants continue to stress that privacy concerns do not only arise in relation to the interception, viewing, use and retention of the *content* of electronic communications. Although it is not intuitively obvious, the ability of computers to match data means that the acquisition and aggregation of "*metadata*"[2] is capable of being at least as intrusive – and often more intrusive - of privacy (Application [§21]; Brown [§§8-14]).

19. The aggregation and matching of metadata allows an extremely detailed picture to be built up about not only a person's communications, but also their movements, habits, religious observance, associates, sexuality and minute aspects of their life. Metadata supplied by, for instance, a mobile telephone, especially if linked to other records, can reveal a person's historical and real-time movements. Such aggregated information is usually far more revealing about a person than the content of particular communications.

20. Since this Application was lodged, the significance of the interception and retention of metadata for interference with private life has been considered and recognised by a number of international bodies:

    20.1. The CJEU in *Digital Rights Ireland* declared the EU's Data Retention Directive to be unlawful, as it constituted a disproportionate interference with the right to privacy of affected persons. The CJEU stressed that "*data, taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them*" (at [§27]). Furthermore, both the Advocate General and the CJEU referred to the fact that one consequence of this is that knowledge that all of one's data is being retained is likely to alter how individuals behave and communicate and create a sense of being

[2] For the purposes of this Application (see Application [§21]), metadata is intended to mean all data about a communication or the maker or recipient of a communication that is not content data.

subject to surveillance that potentially has profound implications for individual freedom within the private sphere.[3]

20.2. The EU Working Party on data protection and privacy (see above at [§12]) recognised that metadata can be more revealing than content data and pointed out that it is easier to analyse than content data:

> "It is also particularly important to note that metadata often yield information more easily than the actual contents of our communications do. They are easy to aggregate and analyse because of their structured nature. Sophisticated computing tools permit the analysis of large datasets to identify embedded patterns and relationships, including personal details, habits and behaviours. This is not the case for the conversations, which can take place in any form or language. Sophisticated computing tools permit the analysis of large datasets to identify embedded patterns and relationships, including personal details, habits and behaviours." (p.5)

20.3. In its report dated 30 June 2014, UNHCHR stated:

> "…it has been suggested that the interception or collection of data about a communication, as opposed to the content of the communication, does not on its own constitute an interference with privacy. From the perspective of the right to privacy, this distinction is not persuasive. The aggregation of information commonly referred to as "metadata" may give an insight into an individual's behaviour, social relationships, private preferences and identity that go [sic] beyond even that conveyed by accessing the content of a private communication."([§19], emphasis added)

20.4. The Special Rapporteur (Terrorism) has expressed the view that the *Weber* criteria apply to metadata just as much as content data – pp.13-14 of his Report, supra, at [§35]). This view corresponds to that of the UN General Assembly's Third Committee.[4]

20.5. UN General Assembly Resolution A/C.3/69/L.26/Rev.1 (26 November 2014) noted that "*certain types of metadata, when aggregated, can reveal personal information and can give an insight into an individual's behaviour, social relationships, private preferences and identity*" (2nd recital, p.3).

20.6. On 5 December 2014, the Office of the Interception of Communications Commissioner, in its Evidence for the Review of Terrorism Legislation by UK's Independent Reviewer of Terrorism Legislation, David Anderson QC ("the Independent Reviewer"), emphasised that "[t]*he volumes and detail contained, especially in traffic data, are at a level not envisaged in 2000*", i.e. when RIPA was enacted. The capacity of modern mobile devices to access data and materials "*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.*" (at [§3.2.8], p.19).

20.7. Finally, the CoE Commissioner has stated that, "*metadata (i.e. recording what links and communications were made in the digital environment, when, by whom,*

[3] The German Constitutional Court has referred to this as the "*diffusely threatening feeling of being watched*", Judgment of 02 March 2010, 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, see https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2010/bvg10-011.html.

[4] As noted in the 4th recital on p.3 of its Resolution A/C.3/69/L.26/Rev.1 (*The right to privacy in the digital age*), dated 27.11.14.

from what location, etc.) can be highly sensitive and revealing, often exposing, for instance, a person's race, gender, religious beliefs, sexual orientation or political and social affiliations." (supra, p.115).[5] But he explained that metadata can also be "*unreliable and can unwittingly lead to discrimination on application of race, gender, religion or nationality. These profiles are constituted in such complex ways that the decisions based on them can be effectively unchallengeable: even those implementing the decisions do not fully comprehend the underlying reasoning*" (supra, p.8).

(c) Breadth of the concept of national security

21. The Applicants stressed (Application [§§105-112 and 147]) the vagueness and breadth of the concept of "*national security*" in English law, which prevents the use of that term from operating as an effective control on the scope of discretion under RIPA. Since the Application was submitted, these concerns have been repeated by other European and national bodies.

i. EU concerns

22. The lack of common understanding of concepts of 'national security' and 'terrorism', and their consequent lack of utility as a robust legal check on state discretion has been noted with concern by a number of EU institutions. On 10 April 2014, the EU Working Party (see above at [12]) adopted an Opinion on surveillance of electronic communications for intelligence and national security purposes (819/14/EN WP 215). It highlighted the fact that, "[t]*here is currently no common* [EU-wide] *understanding of what is meant by national security*" (p.14). The same is true across the Council of Europe.

23. On 19 January 2015, the Committee on Civil Liberties, Justice and Home Affairs (LIBE) of the European Parliament published a report entitled "*National security and secret evidence in legislation and before the courts: exploring the challenges*". The authors expressed the view that, "*the very term 'national security' is nebulously defined across the Member States analysed* [including the UK], *with no national definition meeting legal certainty and "in accordance with the law" standards and a clear risk that the executive and secret services may act arbitrarily*", notably given that "*the conceptual features attributed to th*[e] *term* ['national security'] *remain 'open-ended' even in those Member States with legal frameworks*" (Abstract and p.34).

ii. Council of Europe concerns

24. In his Issues Paper, the CoE Commissioner stressed that the concepts of terrorism and national security "*remain dangerously ill defined*" (p.29). Moreover, the Paper emphasised that:

> "the very question of what legitimately can be said to be covered by the concept of "national security" is justiciable: it should be up to the courts to determine, in the light of international human rights law, what is – and what is not – legitimately covered by the term. Useful guidance on this is provided in the Johannesburg Principles on National Security, Freedom of Expression and Access to Information, drafted by the NGO Article 19 but endorsed by various international forums

[5] See also [§12] of the Explanatory Memorandum of Mr Pieter Omtzigt, rapporteur to the Parliamentary Assembly of the Council of Europe's Committee on Legal Affairs and Human Rights (26 January 2015).

including the UN Special Rapporteur on Freedom of Opinion and Expression. These principles make clear that states can only invoke national security as a reason to interfere with human rights in relation to matters that threaten the very fabric and basic institutions of the nation" (p.19 and see also p.109 and Recommendation 19).

The CoE Commissioner's recommendation was that, even in relation to "*actions of states that relate to the Internet and e-communications* […] *states should only be allowed to invoke national security as a reason to interfere with human rights in relation to matters that threaten the very fabric and basic institutions of the nation*" (pp.19, 24).

iii. Concerns at national level

25. As noted by the CoE Commissioner, it is not only the concept of national security which is nebulous but also the concept of 'terrorism'. Terrorism is a component part of national security. Thus, the *Security Service Act 1989* s1(2) states that the function of the Service is the *"protection of national security, and, in particular its protection against threats from espionage, terrorism and sabotage…"* (Application [§59] (emphasis supplied)). Indeed, in his evidence to the Investigatory Powers Tribunal in the proceedings examined below (see [34] et seq. below), Mr Charles Farr, Director General of the Office for Security and Counter Terrorism of the Home Office, justified warrants obtained under s.8(4) of the Regulation of Investigatory Powers Act 2000 ("**RIPA**") in part by reference to a *"significant and enduring threat from terrorism…. and other national security threats"* [§14]. It follows that any threat from "*terrorism*" is a threat to "*national security*".

26. The definition of "*terrorism*" is set out in s.1 of the *Terrorism Act 2000*[6]. Its breadth and vagueness have been illustrated by recent developments in UK law. The Independent Reviewer[7] has repeatedly drawn attention to the very broad, vague and undefined nature of the concept of 'terrorism' in successive annual reports, criticism now recognised and reflected by the Supreme Court:

    26.1. The Independent Reviewer expressed such concerns in his report dated July 2011 **[Annex 6]** [§§3.2-3.9].

    26.2. In his June 2012 report **[Annex 6]**, he stated that "*the current law allows members of any nationalist or separatist group to be turned into terrorists by virtue of their participation in a lawful armed conflict, however great the provocation and however odious the regime which they have attacked*." [§3.11 also §4.50].

    26.3. In his July 2013 report **[Annex 6]**, the Independent Reviewer concluded that the effect of the definition was, "*to grant unusually wide discretions to all those concerned with the application of the counter-terrorism law, from Ministers*

[6] "*1. (1) In this Act "terrorism" means the use or threat of action where–*
(a) the action falls within subsection (2), (b) the use or threat is designed to influence the government or an international governmental organisation or to intimidate the public or a section of the public, and (c) the use or threat is made for the purpose of advancing a political, religious, racial or ideological cause.
(2) Action falls within this subsection if it– (a) involves serious violence against a person, (b) involves serious damage to property, (c) endangers a person's life, other than that of the person committing the action, Terrorism Act 2000, (d) creates a serious risk to the health or safety of the public or a section of the public, or (e) is designed seriously to interfere with or seriously to disrupt an electronic system."

[7] The Independent Reviewer is appointed to review the Terrorism Acts 2000 and 2006 by s.36 *Terrorism Act 2006*. He also has responsibilities under other statutory provisions.

exercising their power to impose executive orders to police officers deciding whom to arrest or to stop at a port and prosecutors deciding whom to charge" (at [§4.3]).

27. Since this Application was lodged, these criticisms have been cited with approval by the Supreme Court in *R v Gul* [2013] UKSC 64, [2014] AC 1260 (29th October 2013). The Supreme Court (at [§§62-63]) considered that the statutory definition of terrorism was so wide that it was compelled to hold that the provision of support to any non-state armed group or freedom fighter that uses force against the armed forces of a state falls within it, even if the use of force is in resistance to abhorrent acts committed by the agents of that state:

> "62. […] we should record our view that the concerns and suggestions about the width of the statutory definition of terrorism which Mr Anderson has identified in his two reports merit serious consideration. […]
>
> 63. […] The [2000 and 2006 Terrorism] Acts also grant substantial intrusive powers to the police and to immigration officers, including stop and search, which depend on what appears to be a very broad discretion on their part. While the need to bestow wide, even intrusive, powers on the police and other officers in connection with terrorism is understandable, the fact that the powers are so unrestricted and the definition of "terrorism" is so wide means that such powers are probably of even more concern than the prosecutorial powers to which the Acts give rise."(emphasis supplied)

28. These comments are equally apt to the very wide executive powers conferred by RIPA for national security purposes, which include prevention of terrorism.

29. The force of these concerns was well illustrated by the case of *R (David Miranda) v Secretary of State for the Home Department* [2014] 1 WLR 3140 in which terrorism was very broadly defined indeed to encompass the actions of investigatory journalists' associates. In that case, David Miranda, partner of the journalist Glenn Greenwald (who was responsible for a number of the Guardian newspaper stories based on the Snowden material), challenged the legality of his detention under Sch. 7 of the *Terrorism Act 2000* while passing through the UK, and the confiscation from him of files containing material leaked by Edward Snowden. The Sch. 7 power only allows a border officer to stop and question a person, and confiscate certain items, for the "*purpose of determining whether he is concerned in the commission, preparation or instigation of acts of terrorism*": Sch. 7 [§2(1)]. However, the Divisional Court held on 19 February 2014 that this power could be used to detain Mr Miranda and to question him in order to ascertain whether Mr Miranda might hold documents leaked by Edward Snowden, because if he did, he would then be "*concerned in*" preparing the disclosure of documents with the purpose of seeking to "*influence*" a government for political or ideological purposes, which attempted "*influence*" – it was held – would amount to an act of terrorism. Thus, the mere intention to disclose data in order to "*influence*" government is within the concept of terrorism as that term is defined in UK law, even without any use of "*intimidation*" or any violence [§§26-27 and 36].

30. In his July 2014 report **[Annex 6]**, the Independent Reviewer repeated his concern about the effect of the broad definition of terrorism for the fourth time, in the light of this judgment. He said that the judgment "*highlighted the remarkable (and some would say alarming) breadth of the UK's current definition of terrorism*" (at [§4.15]) and seemed to have the consequence that "*the publication (or threatened publication) of words may equally constitute terrorist action*" [§4.16].

Emphasising the potentially wide-ranging effect of this (at [§§4.20-4.22]), the Independent Reviewer particularly stressed that "[t]*o bring activities such as journalism and blogging within the ambit of "terrorism" (even if only when they are practised irresponsibly) encourages the "chilling effect" that can deter even legitimate enquiry and expression in related fields*" [§4.22(c)].

31. These decisions, and the Independent Reviewer's observations, emphasise that statutory restrictions on the interception of communications or the use (etc) of intercepted material by reference to the interest of "*national security*" give an extremely wide discretion to the UKIS and the UK Government and allow the powers to be applied to a very wide array of situations which fall well outside the notion of protecting the UK from terrorism as it is commonly understood.

(d) The Data Retention and Investigatory Powers Act 2014

32. Since this Application was lodged, the *Data Retention and Investigatory Powers Act 2014* ("**the 2014 Act"**) made amendments to RIPA **[Annex 8]**. In particular, s.3 of the 2014 Act provides that the "*economic well-being*" basis for interception in s.5(3) RIPA or the obtaining of communications data pursuant to s.22 RIPA is limited to economic well-being related to state security (as set out in the Interception of Communications Code of Practice at §4.4). Section 3 of the 2014 Act added the words "*in circumstances appearing to the Secretary of State to be relevant to the interests of national security*". This reflects the breadth of the definition of "*national security*" outlined above and the discretion accorded to the Secretary of State in deciding what is in the interests of national security, which can clearly include economic well-being. This will have little, if any, impact on the exercise of the interception powers (see [§§35 and 147] of the Application).[8]

33. Section 6 of the 2014 Act increases the number of reports which the Interception of Communications Commissioner must lay before Parliament. However, the Applicants emphasise that the regularity of such reports is only one aspect of the many weaknesses of the oversight regime (at [§170] of the Application).

(e) Voluntary Disclosures in IPT proceedings on the TEMPORA issue

34. Since this Application was lodged, more is known about TEMPORA as a result of disclosures which the UK Government elected to make during the course of the IPT proceedings. Although the IPT judgments were based upon a series of assumed facts (see 1st IPT Judgment, [§§14-15 and 78] and 2nd IPT Judgment, [§27]), during the course of the IPT proceedings, the UK Government published information about its interception regime under s.8(4) RIPA (Application, [§§68-69]) (hereafter "**s.8(4)**"). This was principally contained in a witness statement dated 16 May 2014 made by Mr Farr **[Annex 3]**.

35. During the course of the IPT proceedings the Government also provided a "*summary of the evidence*" of internal "*arrangements*" which had been adduced in

[8] The definition of "*economic well-being*" in other parts of RIPA, the Investigatory Powers Tribunal Rules, ss.1 & 3 of the *Intelligence Services Act 1994*, and s.1 of the *Security Service Act 1989* have not been similarly amended (see [§§55, 57, 59, 83 and 121 of the Application]).

a confidential closed session of the IPT (see [§§47-48 and 126] of the 1st IPT Judgment and [§30] of the 2nd IPT Judgment).

36. The Applicants emphasise that (1) this information was volunteered by the Government and (2) this information had not previously been made public.

i. Confirmation of the existence of bulk data interception and collection

37. Whilst Mr Farr refused to confirm or deny the existence of the TEMPORA programme [Farr §48], he did acknowledge that interception under s.8(4) *"takes place at the level of interception cables, rather than at the level of individual communications"* [Farr §139] and that *"the only practical way in which the government can ensure that it is able to obtain at least a fraction of the type of communication in which it is interested is to provide for the interception of a large volume of communications, and the subsequent selection of a small fraction of those communications for examination by the application of relevant selectors."* [Farr §149] (emphasis supplied). He also said that it *"involve[s] the interception of volumes of communications and the subsequent performance of a process of selection with respect to those communications to obtain material for further consideration by government agencies."* [Farr §150]

38. Mr Farr stated that the process under s.8(4) is "*similar*" to "*strategic monitoring*" by German intelligence agencies, *"which involves the interception of communications channels as a whole and the subsequent filtering of the intercepted data using selection terms."* [Farr §150].

39. It is thus clear from Mr Farr's evidence that s.8(4) is used to engage in bulk data interception and collection, by reference not to any particular threat but to the nature of the "*communications channel*" on which the data is carried, such as transatlantic fibre optic cables. As explained in the Application, and confirmed by Mr Farr, such intercepted data is then subject to bulk data reduction and searching by "*selector*" or search term.

40. However, the UK Government did not disclose any information about the nature or scope of the process of searching, looking at and using the data intercepted in this way, under a general s.8(4) warrant. Nor was any information provided about what a warrant under s.8(4) might contain or what restrictions might be included within it, save that the IPT noted that s.8(4) warrants "*would be likely to be applied for on a 'generic basis'*" (at 1st IPT Judgment [§101(ii)]).

ii. Bulk interception and collection of "internal" communications

41. A second matter that Mr Farr confirmed in his evidence to the IPT is that the UK's bulk interception and collection regime applies to "internal" communications (i.e. communications between sender and recipient both in the British Islands[9]) as well as "external" communications. Notwithstanding the

[9] See, s. 20 RIPA. For the purposes of UK legislation concerning the interception of communications and the activities of the UKIS, reference is regularly made to "*the British Islands*" rather than the United Kingdom in order to distinguish "internal" and "external" situations (see, e.g. ss.5, 16(2)(a) & (6), and 20 RIPA; ss.1(1)(a), 3(2)(b) ISA; s.1(3)

language of s.8 RIPA, which is restricted to "external" communications, Mr Farr stated [Farr §155] that warrants issued under s.8(4) are treated by UK authorities as authorising them to intercept and collect "internal" communications too. This is because "internal" communications are often routed in whole or part overseas. For example, emails often pass through foreign servers based in countries such as the USA.

42. Mr Farr's evidence as to actual state practice as regards what is capable of interception under a s.8(4) warrant is contrary to the spirit of the UK Government's public statements as to what would be regarded as "internal" and what would be regarded as "external" communications for the purposes of the application of the RIPA regime. During the parliamentary debates on RIPA, a concern was raised about what would be treated as "internal" and what "external" (in the context of email communications). Lord Bassam, a spokesman for the Government expressly stated to the legislature which passed the legislation that email communications between persons in the UK but routed outside of the British Islands would be treated as "internal" communications.[10] This was reflected in the Interception of Communications Code of Practice (2007) [AB/921-962], which states at §5.1 that "external" communications, "*do not include communications both sent and received in the British Islands, even if they pass outside the British Islands en route*"[11]. Moreover, in a written Parliamentary answer to Lord Phillips of Sudbury given on 4 July 2000 **[Annex 7]** as to the operation of (what became) section 16(3) of RIPA, Lord Bassam stated in terms that it "does not authorise the interception of any internal communications beyond the irreducible minimum"; that selectors would be designed to collect "external" communications that fit the descriptions of the certificate and so such selection "is not in practice likely to catch many internal communications" (emphasis added).

43. Mr Farr explains [Farr §152] that notwithstanding these public assurances and the Code of Practice, UK authorities nonetheless treat warrants issued under s.8(4) as authorising them to intercept such – "internal" - communications between sender and recipient in the UK which are routed abroad. He claims that this is authorised by RIPA s.5(6)(a), which states:

> "(6) The conduct authorised by an interception warrant shall be taken to include –
>
> (a) all such conduct (including the interception of communications not identified by the warrant) as it is necessary to undertake in order to do what is expressly authorised or required by the warrant; …"

44. Mr Farr states that since s.8(4) warrants authorise bulk data interception and collection, it is inevitable—and therefore "*necessary*" within the meaning of s.5(6)(a)—that this will result in the interception and collection of "internal" communications routing overseas. He states:

> "There are a number of reasons why as a matter of practice the section 8(4) regime may need to be able to intercept more than simply those communications that may –

SSA). The term "*the British Islands*" includes the Crown dependencies of the Channel Islands (the Bailiwick of Jersey, the Bailiwick of Guernsey (including Alderney, Herm and Sark)) and the Isle of Man (see s.5 and Schedule 1 of the *Interpretation Act 1978*).

[10] Hansard, House of Lords Debates, 12 July 2000, Col 323 (Lord Bassam of Brighton) **[Annex 7]**.

[11] The same statement is also included in the new draft code of practice, which is currently out for consultation, at para 6.5, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/401866/Draft_Interception_of_Communications_Code_of_Practice.pdf

pursuant to section 16 and the certificate in question – be read, looked at or listened to. In particular, internet communications may take any number of routes to get from their sender to recipient. Internal and external communications will be carried together over communications links and it is not at all unusual for internal communications to be routed over international links." [Farr §153]

45. The evidence is that the use which the UK Government considers 'necessary' under s.5(6)(a) RIPA goes far beyond "inevitable" collateral interception. Mr Farr states that the UK Government considers not only interception, but also collection and use of "internal" communications under a s.8(4) warrant to be lawful as long as the "*primary purpose and object*" of a warrant under s.8(4) is the collection of "external" communications [Farr §155].

46. It is therefore clear that, given that the TEMPORA regime collects all available transatlantic data traffic - and contrary to Lord Bassam's assertion that "not … many" internal communications would be caught - a vast amount of "internal" communications will be both *intercepted* by means of s.8(4) warrants and used, subject only to the "*safeguard*" of s.16 RIPA (as to which, see Application [§§145-152]).

47. Since s.8(4) warrants authorise interception of all data travelling on a certain channel, it must mean that all "internal" communications travelling along that path are also intercepted because "*interception under the s.8(4) regime takes place at the level of interception cables, rather than at the level of individual communications*" as noted above. It is also not possible to distinguish between "internal" and "external" communications at the point of interception.[12]

48. Mr Farr says that "*operations are conducted*" in a way which keeps the "*interception*" of "internal" communications to "*the minimum necessary to achieve the objective of intercepting wanted external communications*" [Farr §§139 and 154]. But given the vast scale of "internal" communication which will be intercepted if all communication along a particular channel is 'caught' by a warrant, it is entirely unclear what Mr Farr means by this statement. Nor does he make the same assertion about 'use'. Although according to Mr Farr, some s.8(4) operations can be "*targeted*" to intercept material most likely to be "external" in nature, this remains at the level of operations, it is not required by the domestic legal framework as the UK Government reads it. No explanation is provided relating to this issue. Nor has any relevant internal policy been disclosed, which would – for instance – explain if and how "internal" communications are "*filtered out*" before they are looked at or used, and no information about how the process of data reduction or filtering applies at all.

iii. Expansive definition of "external communications"

49. Another striking admission in Mr Farr's statement relates to the way that the UK Government applies the distinction between "external" and "internal" communications.

[12] The technical aspects of this are usefully explained in a witness statement dated 8 June 2014 served in the IPT proceedings by Mr Eric King, Deputy Director of Privacy International, at [§§7-16] **[Annex 4]**. This feature was also noted by Lord Bassam in the passage cited at [42] above.

50. Mr Farr explains, for the first time, that the UK Government and its intelligence agencies and law enforcement bodies adopt a very broad understanding of "*external communications*". Such communications are treated as the legitimate object of a s.8(4) warrant by the UK Government. His explanation reinforces the Applicants' submission that the scope of the UK's bulk interception regime is far further reaching than had previously been appreciated.

51. Mr Farr sets out the UK Government's view that a person in the UK engages in an "external" communication when they conduct a Google search on their internet browser, use YouTube, post an item on a Facebook page (including their own) or use Twitter. The reason for this, he states, is that such actions are in substance communications between the user and the web servers of those companies, and they will constitute "external" communications when such companies' servers are based overseas. Thus, he says, a Google/YouTube/Facebook/Twitter etc search or communication by a user in the UK and the reply communication of Google etc to the user's computer are regarded by the UK Government as involving two "*external communications*" for the purposes of s.20 RIPA and §5.1 of the Code of Practice (see Farr [§§134-138]).

52. This presumably even extends to a situation where individuals have no intention to communicate with persons abroad (e.g. where Google is used by a UK-based user to search for a UK-based site; or a Facebook user closes their settings to 'friends only' and has friends based only in the UK). In any event, it represents an arbitrary, uncertain and very expansive notion of "external" communications.

53. Nor is this expansive interpretation accessible. Indeed, the Government's Code of Practice, far from indicating that the Government treats the concept of 'external communications' as having the broad scope suggested by Mr Farr, indicates precisely the opposite. As referred to in paragraph [42] above, the Code expressly provides that an email routed on the internet via an overseas country is to be treated as an "internal" communication where both sender and recipient are located in the UK. This reflects the intention of the user and does not depend upon the pure happenstance of the location of the relevant server. The Code of Practice does not address internet communications (other than email) at all, but reading what the Code says about email would lead an internet user to assume that it is the location of the subject and object of the communication which determines whether it is "internal" or "external", rather than the location of the server.

54. Accordingly, an individual user could not reasonably anticipate the interpretation placed on the law suggested by Mr Farr. Indeed, the Applicants note that even technical experts did not appreciate that RIPA operated in this way. Professor Ian Brown, for instance, states that he was surprised to read Mr Farr's explanation.[13]

55. It is very difficult to reconcile Mr Farr's explanation of the approach of the intelligence services in the context of Google, Facebook, Twitter (etc) with what he says about email communications. In relation to email he states:

[13] Ian Brown statement in support of *Privacy International v SSCFA*, 7 June 2014, at [§4] **[Annex 5]**.

> "an email from a person in London to a person in Birmingham will be an internal, not external, communication for the purposes of RIPA and the Code, whether or not it is routed via IP addresses outside the British Islands, because the intended recipient is within the British Islands. The intended recipient is not any of the servers that handle the communication whilst en route (whether that server be located inside, or outside, the British Islands). Indeed, the sender of the email cannot possibly know at the time of sending (and is highly unlikely to have any interest in) how that email is routed, or what servers will handle it on its way to the intended recipient." [Farr §129]

56. Based on this approach—and the Code of Practice being otherwise silent on the application of RIPA to the internet—one would expect that where a person uses the internet but does not intend to communicate with a person outside the United Kingdom this would also be treated as an "internal" communication.

57. The last sentence of [Farr §129] of Mr Farr's statement quoted at [55] above applies with equal force to all internet use, not only sending of emails. By treating "*external communication*" as any communication with a foreign web server, the Government renders the distinction between "external" and "internal" communications entirely arbitrary, since whether a communication is "internal" or "external" does not relate to the *nature* of the communication, or the *conduct* of the persons communicating with each other, but to a factor – the location of the web server in question – which is outside the control of the individual web user and which he or she "*cannot possibly know*". Nor can the way in which communications are categorised for the purposes of deciding what can be lawfully intercepted, looked at or used, meet Article 8 requirements of foreseeability and accessibility, since an internet user has no means of knowing whether a communication will be routed in a way which renders it "internal" or "external" as a matter of domestic law.

iv. Absence of any further information about reduction and selection of bulk intercept material or the transfer of UK intercept material to third parties

58. Mr Farr's statement provides no information about the process of reduction and selection of data. No further information about such matters has been disclosed by the Government.

59. Further, no information has been provided by the UK Government as to the allegations that GCHQ-intercepted material has been provided to third parties, such as the NSA (Application [§§39-40]).

v. Summary of internal arrangements relating to record-keeping and retention periods

60. As noted in [35] above, the Government has voluntarily disclosed a summary of some of the internal arrangements which relate to the process applied to the use of intercepted data, and the length of periods of retention. This summary is set out in [§126] of the 1st IPT judgment.

61. In short:

61.1. Members of the intelligence services who receive unanalysed "*intercepted material*" and related communications data under a s.8(4) warrant "*have*

internal "arrangements" that require a record to be created, explaining why access to the analysed intercepted material is required" before a person is able to access the "*intercepted material*" pursuant to s.16. The internal 'arrangements' only impose a requirement to keep a record of some kind. They do not specify what must be recorded as to the use made of such material. Moreover, the 'arrangements' only apply before a person can gain access to "*intercepted material*. But it is vital to understand that in domestic law, "*intercepted material*" is not all material intercepted under a s.8(4) warrant. It is restrictively defined, in s.20(1) RIPA, to mean "*the contents of any communications intercepted by an interception to which the warrant relates*" (emphasis supplied). The internal arrangements referred to therefore do not apply if what is to be examined is communications metadata, including e.g. information about the identity of a person making a communication and who received it, the location of the communication, information about the device used, its operating system and hardware, or the identity of websites visited (etc) (all of which is not content data).[14]

61.2. Secondly, the "*internal "arrangements""* specify, or require to be determined, maximum retention periods for different categories of data – including both "intercepted material" (content) and communications data – in order to "*reflect the nature and intrusiveness of the particular data at issue*". However, the internal arrangements, the retention periods and the criteria of intrusiveness are not disclosed; save that the retention periods are said to be "*normally no longer*" than a maximum of 2 years and "*may be*" significantly shorter. Material may also be retained for longer than the "normal" maximum period if "*prior authorisation*" has been obtained from a "*senior official within the particular intelligence service at issue on the basis that the continued retention of the particular data at issue has been assessed to be necessary and proportionate*". It is not clear what influence technological limitations have had on these periods and thus whether, as storage capacity increases, the quantity and duration of such storage will also do so.

61.3. Thirdly, no disclosures have been made by the Government in relation to restrictions or procedures applicable to the provision of "intercepted material" (ie content) or – indeed – communications data (ie metadata) to third parties such as the NSA. Nor indeed is there any disclosure as to the extent to which the NSA can specify or suggest selectors for the use of such material. There is therefore no published or publicly available guidance on how such data access occurs or what uses can be made of it by a third party. NSA disclosures confirm direct access to this data and the specification of search terms[15] (Application [§§6.3, 39, 177.6]).

(f) Disclosure by the Intelligence and Security Committee of Parliament

62. In a report published on 25 November 2014 into the distinct issue of the murder of Fusilier Lee Rigby outside an army barracks in London (by killers describing

[14] The arrangements also on their face do not apply to intercepted content from "internal" communications. This is because s.8(4) warrants do not relate to such communications and therefore such material is not "intercepted material". This would clearly leave a further substantial gap in the internal arrangements.
[15] See Second Witness Statement of Cindy Cohn dated 2 March 2015, paras [13], [16] **[Annex 2]**.

themselves as motivated by Islamist ideology), the UK Parliament's Intelligence and Security Committee ("**ISC**") provided the following public account of the UK Government's interception capability:

> "GCHQ [] has access to communications as they move over the internet via the major internet cables. This provides the capability to intercept a small proportion of internet traffic: in theory, GCHQ can access around ***% of global internet traffic and approximately ***% of internet traffic entering or leaving the UK. However, the resources required to process the vast quantity of data involved mean that, at any one time, GCHQ can only process approximately *** of what they can access. This means that the odds of collecting the content of the communications of an individual who is not specifically being targeted are *** – even if their communications have met other selection criteria they are ***". [*** denotes redacted material].

63. A member of the ISC, Lord Butler, later stated that the Committee had intended to put a description of GCHQ's capability (but not the TEMPORA codename) into the public domain in the face of the Government's repeated refusal to confirm or deny the same.[16]

(g) Further relevant disclosures from the Snowden files

64. There have been further disclosures in the press since the Application was filed relating to the challenge to the TEMPORA regime. These include:

64.1. Further allegations that GCHQ intercepted the communications of foreign leaders and diplomats, allegedly for trade reasons. An internal GCHQ document refers to the fact that GCHQ exploited the use of smartphones by diplomatic targets at the G20 summit in 2009 and was able to access their emails, "*reading them before the* [targets] *do*" (e.g. "*GCHQ intercepted foreign politicians' communications at G20 summits*", The Guardian, 17 June 2013 [AB/630-634]). Further reports have now revealed surveillance by the US and UK intelligence services of more than 1000 political targets between 2008 and 2011 in 60 countries, including foreign leaders such as the then Israeli Prime Minister, Ehud Olmert, the vice President of the European Commission, Joaquin Almunia and the Federal Chancellor of Germany, Angela Merkel. The NSA and GCHQ were also reported to have spied on several UN Missions in Geneva, including UNICEF, the UN Institute for Disarmament Research and Medecins du Monde as well as major telecommunications providers whose clients include the European Union's institutions (e.g. "*New leak shows US, UK spying on heads of state, international orgs*" Al-Jazeera America, 20 December 2013; "*Belgacom Attack: Britain's GCHQ Hacked Belgian Telecoms Firm*", 20 September 2013).

64.2. Further documents explaining the scale of the TEMPORA programme and the NSA's access to it have been published, showing the scale of this programme.[17] For example, an NSA document dated 19 September 2012 describes TEMPORA as "*more than 10 times larger than the next biggest XKEYSCORE [the NSA's computer system for searching and analysing intercepted internet data] …This massive site [TEMPORA] uses over 1000 machines to process and make available to analysts more than 40 billion pieces of*

[16] "*Thatcher and Blair Cabinet Secretary: Intelligence committee has 'helped' public by confirming GCHQ's internet tap 'Tempora' powers*" The Bureau of Investigative Journalism, 11 January 2015, M. Newman.
[17] See Second Witness Statement of Cindy Cohn, para [13] **[Annex 2]**.

content a day." It describes TEMPORA as "*GCHQ's 'Internet buffer' which exploits the most valuable Internet links available to GCHQ*" (Der Spiegel, 18 June 2014, "*New NSA Revelations: Inside Snowden's Germany File*").

64.3. There have been further allegations of surveillance of NGOs and other public interest entities[18] and specific issues have been raised which inevitably arise if there insufficient safeguards on mass interception of data – such as (for example) as to the surveillance of confidential/journalistic material as well as legally professionally privileged material.[19] Indeed, it was recently reported that the Government has now conceded that the UKIS' policies and procedures governing the handling of legally privileged communications, adopted since January 2010, did not meet the requirements of article 8 ECHR[20].

(h) Judgment of the IPT on the TEMPORA issue

65. In its first judgment on 5 December 2014 **[Annex 9]**, the IPT held that the interception of communications under s.8(4) RIPA was compatible with Article 8 of the ECHR.

66. In reaching this conclusion, the IPT addressed a series of four issues which it had itself formulated [1st IPT Judgment §80]. The IPT reasoned as follows:

66.1. Firstly, the IPT asked whether uncertainty as to the scope of s.8(4) and in particular its application to "*external communications*" led to a violation of Article 8. It reasoned that:

(1) it was foreseen at the time RIPA was enacted that some "internal" communications would be intercepted under s.8(4) because of the intermingling of internet communications via email;

(2) it was clear in its view from the statutory regime[21] that certain internet uses such as use of Google search and posting messages on Facebook which are read by persons overseas were 'external'. Although other internet uses (which were less clear) created levels of uncertainty, these were considered to be of "*very limited ambit*"; and

(3) there had not been any "*radical change*" in internet use such as to transform the s.8(4) regime.

The IPT concluded that no difference of view as to the scope of s.8(4) rendered it contrary to Article 8 [1st IPT Judgment §§80, and 100-102]. The IPT chose to focus narrowly on the extent of uncertainty as to the application of s.8(4) to "internal" communications. Its conclusion was that s.8(4) is sufficiently clear and precise in its scope of operation to satisfy Article 8.

66.2. Secondly, the IPT found that to the extent that there need to be some safeguards in place in order to render the bulk interception of data in

[18] See, for instance, the disclosures on 20.12.13 set out in the attached timeline **[Annex 1]**.
[19] See, for instance, the disclosures on 18.02.14, 02.09.14, 06.10.14, 06.10.14, 12.10.14, 06.11.14 and 09.12.14 set out in the timeline **[Annex 1]**.
[20] In particular, that safeguards against misuse were not sufficiently public to comply with the requirement of legality - The Guardian, 18 February 2015.
[21] The effect of RIPA in these cases was said to have been accepted by the claimants.

accordance with law for the purposes of Article 8, s.16 is sufficient. It accepted that s.16 only imposes restrictions on looking at and using the "*intercepted material*" of persons in the UK. However, "i*ntercepted material*" is given a narrow definition (by s.20(1) RIPA, see [61.1] above) to mean the content of such person's communications. Thus s.16 imposes no restrictions at all on the review and use of all other types of data derived from the intercepted communications of persons in the UK, including metadata. Indeed, the IPT held that it would be necessary to review some of this wider information in order to establish if a person was in the British Islands (which is the statutory trigger necessary to create a restriction on use of content data), and held that the fact that this would be necessary justified the absence of any restriction on reviewing or using such non-content data [1st IPT Judgment §114].

66.3. This was in an important failing in the IPT's reasoning. The IPT failed to recognise that there are real privacy concerns – and consequently a real need for legal safeguards – about the use of non-content data (for the reasons set out at [18-20] above). Its reasoning in relation to non-content data assumed that that s.16 establishes an appropriate safeguard for s.8(4) warrants.

66.4. Nor did the IPT recognise that the s.16 protections in relation to content data apply only after machine analysis and application of selectors. Content data referable to persons inside and outside the British Islands is therefore intercepted, buffered and stored and searched using selectors and thus 'used' *before* the protections of s.16 are even engaged. Such searching and use is carried out by an (unknown) automated process, which could for example include algorithms and criteria relating to status, ethnicity, religious views or political opinion which would raise serious Article 8 concerns and require legal regulation.

66.5. The IPT also did not consider there to be any breach of Article 8 in relation to persons outside the British Islands despite the fact that s.16 RIPA will not apply to such persons except if examination of their communications is "*referable to an individual*" in the British Islands.

66.6. Thirdly, the IPT then turned to consider whether, leaving s.16 aside, there is sufficient clarity and prescription in RIPA ss.8(4) and 15 to comply with the requirements that infringements of private life are "*in accordance with law*". It held that there was. It reasoned as follows:

(1) Relying on this Court's acceptance in *Kennedy v United Kingdom* that the notion of "*national security*" under UK law was clear and imposed a control on the exercise of discretion and, following *Weber* and *Liberty*, that the legislation thus contained a sufficient description of the conduct which justifies interception even though GCHQ intercepts all communications passing on certain channels through the British Islands, the vast majority of which have nothing to do with national security. Such bulk collection is, it said, "*acceptable and inevitable*" [1st IPT Judgment §116(i), (ii), (iii)].

(2) The discretion of the intelligence agencies as to use of "*intercepted material*" under s.8(4) is also sufficiently prescribed by §5 of the Code of Practice. The IPT relied on this Court's judgment in *Liberty v United Kingdom* (2009) 48 EHRR 1 in which the pre-RIPA regime for intercepting "*external communications*" had been found in breach of Article 8 for conferring a "*virtually unfettered*" discretion on the executive, but said it drew a "*strong inference*" that this Court had indicated that with the Code of Practice in place the regime was Article 8 compliant [1st IPT Judgment §§90 and §116(ii)].[22]

(3) The IPT found that *Weber v Germany* did not impose a requirement for search terms to be indicated [1st IPT Judgment §116(v)] and concluded that *Kennedy* had held that it was unnecessary for there to be judicial authorisation given oversight by the Interception of Communications Commissioner [1st IPT Judgment §116(vi)].

(4) It also held that there are sufficient restrictions on the duration of the interception, examination, use and storage, disclosure, and destruction of intercepted material. The IPT reasoned:

a. That this Court had recognised the sufficiency of the protections set out in s.15 of RIPA dealing with examination, use, retention and disclosure in *Kennedy v UK* and the IPT simply read those findings across to s.8(4) notwithstanding that *Kennedy* was concerned with warrants targeted at specific individuals or premises. The IPT said that it would not reconsider the findings in *Kennedy* [1st IPT Judgment §§123-124].

b. The IPT referred to the further voluntary disclosures set out above [60-61] relating to record-keeping and retention lengths. It held that it was entitled to do so on the basis that "*undisclosed administrative arrangements, which by definition can be changed by the Executive without reference to Parliament, can be taken into account, provided that what is disclosed indicates the scope of the discretion and the manner of its exercise*" (emphasis in original). It also emphasised that the Code of Conduct refers to arrangements not contained therein and that in *Liberty v United Kingdom* this Court had only required disclosure of "*certain details*". Furthermore, there is a system of oversight of the "*internal arrangements*" which this Court has approved in *Liberty* and *Kennedy* [1st IPT Judgment §129].

c. That on the basis of "*what we saw and heard at the closed hearings, and the further Disclosure set out above*," the UKIS were not able to build-up a database of communications data about individuals obtained under a s.8(4) warrants, as had been claimed by the claimants [1st IPT Judgment §139]. In reaching this conclusion, the IPT expressly relied upon what it had seen in secret, closed, hearings to which neither the claimants in that case, nor the

[22] It considered that §5 of the Code of Conduct was "*impressive*" and "*satisfactory*" (1st IPT Judgment [§116(iv)]).

applicants in this Application, nor any other person have had or can obtain access. This conclusion is however contradicted by the Snowden disclosures regarding TEMPORA, which make clear that it was by far the largest searchable ("XKEYSCORE") database available to NSA operators globally (see [64.2] above)[23].

66.7. Fourthly, the IPT addressed whether the regime was indirectly discriminatory on grounds of race, nationality and national origin because the protections of s.16 only apply to persons in the British Islands. It held that the indirect discrimination was justified because "*it is harder to investigate terrorism and crime abroad, and difficult if not impossible to provide a case for a certificate under s.16(3) in every case*". In relation to a target abroad there "*might not be any or any sufficient information for a section 16(3) certificate*" and it would "*radically undermine the efficacy of the section 8(4) regime*" (1st IPT Judgment [§§147-148]).

66.8. As to this fourth issue, the IPT recalled that s.16(3) enables the Secretary of State to certify that the examination of material relating to an individual for the purpose of identifying material contained in communications sent by him, is necessary for the purposes of national security, preventing or detecting serious crime or safeguarding economic well-being. In dismissing the discrimination challenge, the IPT accepted that the content of communications made by persons outside the British Islands are often reviewed despite the fact that there would be insufficient evidence to support a certificate on the s.16(3) grounds. This reveals that the communications of persons outside the UK can be, and are, intercepted and examined on the basis of a general, abstract, national security justification rather than any national security justification which is specific to the person whose communications are intercepted and examined.

67. It is apparent from this analysis of the IPT's judgment that it took a relatively technical approach, focusing, for example, on certain sub-issues within the broader Article 8 issue, such as the degree of uncertainty in application of s.8(4) warrants to "internal" communications.

68. Furthermore, the IPT:

68.1. Did not address in substance key issues raised by this Application, such as (a) the degree of discretion conferred by the notion of "*national security*" (which this Application asks the Court to reconsider in the light of recent developments), and (b) whether the regime satisfies the requirement of proportionality (it addressed only the "according to law" requirement)[24] and (c) whether the provision of data intercepted by the UKIS to third parties is sufficiently regulated; and

68.2. Failed properly to appreciate the implications of interception and use of metadata for interference with privacy; and

[23] See Second Witness Statement of Cindy Cohn, para [13] **[Annex 2]**.
[24] The IPT will consider the proportionality of the interception of communications in particular instances relating to the claimants in future closed proceedings. The proportionality of the regime as a whole was not considered.

68.3. Rested its determination on the key issues on interpretations of the case law of this Court, in particular *Liberty*, *Kennedy* and *Weber*.

69. As to the IPT's failure to appreciate the importance of use of metadata as an interference with privacy, the Applicants' observations are set out at [18-20 and 61.1] above.

70. As to the IPT's analysis of this Court's reasoning in its earlier case-law, this was not correct. For example:

70.1. This Court's judgment in *Liberty* did not endorse the RIPA s.8(4) regime or the Code of Practice. On the contrary, it points strongly to the insufficiency of the legal safeguards (Application [§§153ff]).

70.2. Far from allowing for secret arrangements to be relied upon to satisfy Article 8, this Court's case law makes clear that safeguards must be set down in published law (Application [§143]).

70.3. This Court's judgment in *Kennedy* only approved the protections under ss.8, 9 and 15 of RIPA in the context of targeted warrants directed at particular individuals or premises in the British Isles. This cannot be read-across to warrants authorising interception, "*at the level of interception cables, rather than at the level of individual communications*", and "*likely to be applied for on a 'generic basis'*". In this context, the notional protections are largely illusory because they apply to such extremely broad categories of material defined only by the route it takes, rather than material about particular targeted individuals (Application [§§145-149]).

71. Further, the Court was, with respect, in error in *Kennedy* in ascribing to UK law a definition of national security far narrower than that which actually exists, for reasons explained in the Application (at [§§105-112 and 147.3]. See also [21-32] above. In the light of the material in this application, the Court is respectfully invited to reconsider that aspect of its reasoning in *Kennedy*.

(i) Updated Conclusion on the TEMPORA issue

72. In the light of the developments referred to above, the Applicants submit that:

72.1. There is now further evidence that GCHQ operates a bulk data interception and collection programme under warrants issued under s.8(4) of RIPA. Under the TEMPORA regime, GCHQ intercepts and stores all communications passing on submarine fibre-optic cables from the British Islands, whether those communications are between individuals in the British Islands or not and including all internet activity with foreign web servers or routing overseas or from overseas via the British Islands. This constitutes a significant proportion of the communications and, in particular, internet use of Europe, the United States and the rest of the World. They are not simply searched passively, but buffered and stored for the purpose of more detailed search and analysis

72.2. Such a dramatic interception regime is authorised under s.8(4) on the basis that the Secretary of State has certified categories of "*external communications*" as being necessary to "*examine*" for the purposes of national security, fighting serious crime or safeguarding economic wellbeing, and therefore the requirements for targeted interception contained in RIPA ss.8(1) and (2) are dis-applied. In other words, it is considered necessary to intercept the communications of all in order to combat the few.

72.3. This interception regime goes far beyond what was envisaged when RIPA was enacted (see [42] above); the intention to conduct such wide-ranging activities is not sufficiently clear from the terms of that Act or the guidance provided under it; the regime does not recognise the implications for private life of interception and use of metadata; and there is no adequate or ascertainable protective mechanism available as a check on exorbitant or arbitrary use of the power.

72.4. Indeed, it is not clearly apparent on the face of RIPA (or the Code) that this regime is used for the object of intercepting and examining such matters as Google or YouTube searches, tweets and Facebook posts. Given the distinction which the legislation draws between "internal" and "external" communications, individuals within the British Islands would expect that interception with the object of obtaining such information on the part of the UKIS would require a targeted warrant under s.8(1) of RIPA.

72.5. However, it has emerged from the IPT proceedings that once a certificate is in place under s.8(4), there are no restrictions at all in statute or any published policy which limit the scope of the interception—indeed, the point of the regime is to intercept everything passing along a particular fibre-optic cable. Further, there are, with one exception, no restrictions set out in RIPA or the Code of Conduct or any other published source which places a limit on what may be inspected other than the fact that it must be regarded as necessary for national security, serious crime or economic well-being purposes. Similarly, there appear to be no restrictions to transfers of the data intercepted to other parties such as the NSA, or its use by them.

72.6. The exception is the restriction set out in s.16 of RIPA. But this section is inadequate:

(1) In respect of persons in the British Islands, it only restricts the ability of the UKIS to look at the content of communications and has no application to examination of metadata about an individual of interest, which is likely to be a far more revealing intelligence tool;

(2) It has no application to persons outside the British Islands, whose communications can be targeted and trawled at will on national security (etc.) grounds;

(3) It only protects persons who are the subject of interest and not the people they are communicating with, even if they are in the British Islands, and

(4) It does not preclude examination of content material where the Secretary of State certifies this is necessary for the purpose of "*national security*".

72.7. For the reasons explained in the Application [§§149-150] the product of a s.8(4) warrant can be used for a very broad array of purposes and held even if it is unlikely to become necessary for those purposes. These include use for other functions of any of the intelligence services, such as supporting the police in the investigation of serious crime.[25] The data can also be surrendered to a third country merely on the basis that correspondingly broad conditions apply under the law or practice of the foreign country on the use and retention of the information as apply under RIPA (and indeed there is evidence that this has occurred on a substantial scale [Application §§39-40]). Moreover, the Secretary of State can, in his or her discretion, permit the supply of intercepted material even in the absence of corresponding legal rules: ss.15(6)(a)-(7)(a)).

72.8. As noted in §§60-61 above, since this Application was drafted, the UK Government has disclosed policies that retention periods for intercept product under s.8(4) will be "*normally no longer than 2 years*" before they are destroyed. These periods are subject to extension, and to differentiation depending on sensitivity of particular forms of data ([§61.2] above). Such internal policies are insufficient to comply with Article 8 requirements of legality: (a) they apply only to lengths of retention, (b) they are vague – there is, e.g., no specificity as to the lengths of time information of particular types is retained or in which circumstances they might be retained for longer periods, (c) they are set out in only partially disclosed "*internal arrangements*", not published law and are subject to unannounced change by the Executive.

72.9. As such, the information disclosed since the proceedings reinforces the strength of the submission that the TEMPORA regime violates Article 8 ECHR.

PART III: THE PRISM ISSUE: UPDATE (Application [§§119-139])

(a) US Developments

73. Developments in the United States since the Application was filed are addressed in a supplementary updating witness statement by Cindy Cohn of the Electronic Frontier Foundation **[Annex 2]**. In short, Ms Cohn concludes that while US legislation has in some cases been altered to restrict access of US intelligence services to the data of "US persons", the same cannot be said for the bulk surveillance of persons outside the US.

[25] S.19(2)-(5) of the *Counter-Terrorism Act 2008*; Mr Farr states: "[…t]his means, for example, that intelligence that is obtained by the Security Service for national security purposes can as appropriate be subsequently used by the Security Service to support the activities of the police in the prevention and detection of serious crime. This degree of operational flexibility regarding the use of intelligence is necessary not least because of the overlap in practice between the various statutory functions of the Intelligence Services, and the fact that a given item of intelligence may be of relevance to more than just the particular purpose for which it was first acquired." [Farr §50]

(b) International bodies

74. The materials referred to in [6-17] above are also of relevance to the PRISM issue. Specific reference is also made to the UNHCHR's report, which stated:

> "30. The requirement of accessibility is also relevant when assessing the emerging practice of States to outsource surveillance tasks to others. There is credible information to suggest that some Governments systematically have routed data collection and analytical tasks through jurisdictions with weaker safeguards for privacy. Reportedly, some Governments have operated a transnational network of intelligence agencies through interlocking legal loopholes, involving the coordination of surveillance practice to outflank the protections provided by domestic legal regimes. Such practice arguably fails the test of lawfulness because, as some contributions for the present report pointed out, it makes the operation of the surveillance regime unforeseeable for those affected by it." ([§30] p.10)

(c) Voluntary Disclosure

75. In the IPT proceedings, the UK Government made voluntary disclosure of the following information about the internal arrangements within the intelligence services for use of intercepted communications obtained by foreign agencies (1st IPT Judgment [§47]):

> "1. A request may only be made by the Intelligence Services to the government of a country or territory outside the United Kingdom for unanalysed intercepted communications (and associated communications data), otherwise than in accordance with an international mutual legal assistance agreement, if either:
>
> a. a relevant interception warrant under the Regulation of Investigatory Powers Act 2000 ("RIPA") has already been issued by the Secretary of State, the assistance of the foreign government is necessary to obtain the communications at issue because they cannot be obtained under the relevant RIPA interception warrant and it is necessary and proportionate for the Intelligence Services to obtain those communications; or
> b. making the request for the communications at issue in the absence of a relevant RIPA interception warrant does not amount to a deliberate circumvention of RIPA or otherwise contravene the principle established in *Padfield v. Minister of Agriculture, Fisheries and Food* [1968] AC 997[26] (for example, because it is not technically feasible to obtain the communications via RIPA interception), and it is necessary and proportionate for the Intelligence Services to obtain those communications.
>
> In these circumstances, the question whether the request should be made would be considered and decided upon by the Secretary of State personally. For these purposes a "relevant RIPA interception warrant" means either (i) a s8(1) warrant in relation to the target at issue; (ii) a s8(4) warrant and an accompanying certificate which includes one or more "descriptions of intercepted material" (within the meaning of s8(4)(b) of RIPA) covering the target's communications, together with an appropriate s16(3) modification (for individuals known to be within the British Islands); or (iii) a s8(4) warrant and accompanying certificate which includes one or more "descriptions of intercepted material" covering the target's communications (for other individuals). The reference to a "warrant for interception, signed by a Minister" being "already in place" in the ISC's Statement of 17 July 2013 should be understood in these terms. (Given sub-paragraph (b), and as previously submitted in open, a RIPA interception

[26] This establishes the public law principle that public powers must be exercised for the purposes for which they were conferred.

warrant is not as a matter of law required in all cases in which unanalysed intercepted communications might be sought from a foreign government.)

2. Where the Intelligence Services receive intercepted communications content or communications data from the government of a country or territory outside the United Kingdom, irrespective whether it is / they are solicited or unsolicited, whether the content is analysed or unanalysed, or whether or not the communications data are associated with the content of communications, the communications content and data are, pursuant to internal "arrangements", subject to the same internal rules and safeguards as the same categories of content or data, when they are obtained directly by the Intelligence Services as a result of interception under RIPA."

76. The following additional disclosure was provided by the UK Government (1st IPT Judgment [§48]):

> "The US Government has publicly acknowledged that the Prism system and Upstream programme, undertaken in accordance with Section 702 of the Foreign Intelligence Surveillance Act, permit the acquisition of communications to, from, or about specific tasked selectors associated with non-US persons who are reasonably believed to be located outside the United States in order to acquire foreign intelligence information. To the extent that the Intelligence Services are permitted by the US Government to make requests for material obtained under the Prism system (and/or on the Claimants' case, pursuant to the Upstream programme), those requests may only be made for unanalysed intercepted communications (and associated communications data) acquired in this way."

77. The disclosure also recorded the UK Government's position as to a request made in the circumstances set out in paragraph 1(b) of the disclosure, namely that "[a]*ny such request would only be made in exceptional circumstances, and has not occurred as at the date of this statement.*" (ibid.)

78. It was common ground between the parties in the IPT proceedings that RIPA does not apply to receipt of intercepted communications, including where that included "*intercepted product of an e-mail which could have been sent and/or received in the United Kingdom*" (1st IPT Judgment [§17]).

(d) The IPT Judgments

79. The IPT held that the disclosed information was a clear "*signpost*" as to what was contained in other, secret, arrangements which it had considered in 'Closed' hearings to which the claimants had not been permitted access (1st IPT Judgment [§50(i)]).

80. The IPT was satisfied that the disclosures were sufficient to satisfy the "*in accordance with law*" requirement under Article 8, with one exception. This related to the failure of the arrangements to require that s.16 RIPA be applied by analogy if a request was made under paragraph 1(b) (1st IPT Judgment [§§53-55]).

81. In reaching this conclusion, the IPT reasoned that the *Weber* criteria (Application [§128]) do not apply to the receipt of information by the UKIS with full force, but a "*lower level*" of protection is warranted (1st IPT Judgment [§§25, 34-37]).

82. At its first hearing, the IPT reserved the question of the application of RIPA by analogy to paragraph 1(b) situations and, more significantly, it reserved the question of whether there had been compliance with Article 8 before the disclosures were made. Before the second IPT hearing took place, the Government undertook that if any request of an untargeted nature for intercept material was made under paragraph 1(b), it would not examine any communications so obtained according to factors set out in s.16(2)(a) and (b) of RIPA unless the Secretary of State had personally considered and approved the examination of those communications by reference to such factors (2nd IPT Judgment [§30]).

83. In a second judgment delivered on 6 February 2015 **[Annex 10]** the IPT held that:

    83.1. Prior to the Government's disclosures about how it approached use of third-party foreign state intercept material, there had been a breach of Article 8 because there had not been "*adequate signposting*" of the fact that the RIPA protections were applied by analogy to data received from foreign partners (2nd IPT Judgment [§§20-21]).

    83.2. That in the light of the further undertaking given by the Secretary of State, the regime now fully complied with Article 8 although it had not done so previously (ibid, [§22]).

(e) Updated Conclusions on the PRISM Issue

84. The Applicants submit that there has clearly been a historic breach of Article 8 of the Convention, which this Court should acknowledge. Moreover, even after the Government's disclosures, there are inadequate safeguards to comply with Article 8 in respect of receipt and use of PRISM material. For all the reasons set out in the Application and above in relation to the TEMPORA issue, the fact that the RIPA regime is applied by "*analogy*" does not satisfy the requirements of Article 8. The regime is not sufficiently protective in relation to material intercepted by UKIS and it is not sufficiently protective in relation to material obtained by foreign agencies and used by UKIS either. It boils down to a requirement that material received by UKIS can be used for any purpose deemed to be in the interests of national security, fighting serious crime or for the economic well-being of the country, with limited further protections for review of the content of communications of persons in the UK analogous to those under RIPA s.16.

85. Furthermore, the "internal arrangements" do not have the character or quality of law for Article 8 purposes:

    85.1. The type of internal arrangements relied upon by UK Government are (1) established by the executive agency in question and are not democratically or independently established, (2) are a matter of internal policy and thus subject to change and a lower standard of enforceability through the courts, and (3) are not published or accessible, especially where - as here - only "gists" are supplied. It is clear from *Weber* that to have the requisite qualities of 'law', the terms of such safeguards must be adequately specified in statute law, not recorded in summaries of internal policies

recorded in a legal judgment. This ensures that the law is properly accessible and can only be changed by open and democratic process.

85.2. The reason why the IPT accepted such "gists" of internal arrangements as being sufficient was because it applied a "*lower level*" of protection to the receipt of intercepted material than that which it considered necessary for the interception of communications directly by the UKIS. It is hard to see why use by UKIS of material intercepted by foreign state agencies is less invasive of privacy than the use of the same material if it happens to have been intercepted by UKIS themselves. The IPT failed to appreciate (1) that the level of intrusion and risk to privacy is precisely the same in respect of the obtaining and use of the material, whether it comes from interception done by the UKIS, at their behest from private contractors or from a foreign intelligence service; (2) the further risks identified by the UNHCHR (at [74] above) and the Committee on Legal Affairs and Human Rights (at [16] above) of 'outsourcing' of interception. The appropriate standard must be that identified by this Court in *Weber*. Indeed, as noted above, the UN Special Rapporteur (Terrorism) and the UN General Assembly's Third Committee appear to treat the *Weber* criteria as the only relevant reference point (see [§20.4] above).

PART IV: EXHAUSTION OF DOMESTIC REMEDIES

86. The Applicants anticipate that the UK Government will argue that the fact these matters were considered by the IPT demonstrates that there was an adequate domestic remedy.

87. However, the two judgments of the IPT do not affect the Applicants' analysis of the absence of effective domestic remedies or question of exhaustion of remedies addressed in the Application at [§§179-190], for the following reasons:

87.1. First, this Court held in *Kennedy* that it is not necessary for a person making a general challenge to the interception regime (as opposed to a specific complaint about interception) to first complain to the IPT. The Applicants are entitled to rely on that case. The Court has held on many occasions that the assessment as to whether domestic remedies have been exhausted is normally carried out by reference to the point in time when an Application is lodged. It would undermine legal certainty if an applicant was not able to rely on a judgment such as that in *Kennedy* in lodging a complaint with this Court and would mean that Applicants first have to resort to domestic processes even where the Court has previously held that this is not required. Whatever may be the position in the future, the IPT proceedings therefore cannot affect the admissibility of this application.

87.2. Secondly, and in any event, the criticisms of the IPT process contained in *Kennedy* remain entirely valid:

(1) Had the IPT upheld rather than dismissed the claims that the domestic regime is in breach of Article 8, it had no ability to grant a remedy because (a) it is not able to grant a declaration of incompatibility under the HRA (Application [§186]), and (b) a

declaration of incompatibility does not in any event amount to an effective remedy (Application [§187], relying on the established principles in *Burden v UK* (2008) 47 E.H.R.R. 38). As the Court noted in *Kennedy*, the "*tribunal did not have the power to annul any of the RIPA provisions or to find any interception arising under RIPA to be unlawful*" [§109]. It is telling that in relation to the faults found with the interception regime before the further disclosures were made by the Government, the IPT did no more than grant a declaration that the regime had not been compliant with Article 8.

(2) *Burden* remains good law, so the principle in *Kennedy* still stands. Although the Grand Chamber in *Burden* noted that "*it cannot be excluded that at some time in the future the practice of giving effect to the national courts' declarations of incompatibility by amendment of the legislation is so certain as to indicate that s.4 of the Human Rights Act is to be interpreted as imposing a binding obligation*" [§43], there has been no such practice. As a matter of domestic law, UK courts have no power to provide an effective remedy against breaches of the Convention if these are contained in primary legislation which cannot be read compatibly with it. Given the dualist system of British law (in which Courts cannot directly apply unincorporated terms of international law), the limited scope of s.4 *Human Rights Act 1998* and the fact that Article 13 ECHR is not separately incorporated into domestic law, the most a UK court can do in the face of legislation which breaches the Convention is to declare that there is such an incompatibility. They cannot require the law to be changed, disapplied, or to order any other form of just satisfaction. Indeed, the UK's Supreme Court recently declined to make a further declaration of incompatibility in a case in which this Court had declared a provision in electoral legislation to breach Article 3 Protocol 1, and following which the domestic courts in an earlier case had declared that provision incompatible with the Convention. They declined to do so on the basis that, since the legislature was aware of the Court's view from its earlier declaration, to do so would serve no further purpose, and it was now a matter for the UK Parliament (as a matter of domestic law) to decide whether to comply with the Convention (see *R(Chester) v Secretary of State for Justice* [2013] UKSC 63, [2014] AC 271, pp.303F-305E per Lord Mance at [§§39-42].

(3) The Court of Appeal has held that the IPT is not a remedy that needs to be exhausted before domestic legal proceedings are pursued: *AJA & Ors v Commissioner of Police for the Metropolis & Ors* [2013] EWCA Civ 1342. The Court noted the shortcomings of the IPT's procedure – which it described as "*distinctly more restrictive than that of the court for obvious reasons: for example, oral hearings before the IPT are discretionary and may take place in the absence of the applicants; applicants have no right to the disclosure of evidence relied on by the opposing party or to know the case against them; there is no right to cross-examine opposing witnesses or to representation or funded representation; there is no right to a reasoned judgment and no right of appeal*" (at [§§54 and 57]) – and noting the limited potential remedies available to affected persons: "*the decision of*

the IPT will amount to little more than a "yes" or "no". It is difficult to see how such a decision will assist the court" (at [§56]).

(4) The disclosures made in the course of the IPT proceedings were made voluntarily. The IPT's Rules prohibit the IPT from disclosing any Government material without the Government's consent: IPT Rules rr.6(2)-(7). Therefore the fact that the disclosures were made does not affect the analysis of the powers of the IPT.

(5) In respect of both its findings on the TEMPORA issue [65-66 above] and the PRISM issue [79-83 above], the IPT relied materially on closed material that it had considered which was not disclosed to the claimants.

88. This point is in any event now academic, since the issues in these proceedings have been ventilated before the IPT. In the unusual circumstances of this case, this Court can be confident that the outcome of the posited alternative remedy would not have provided the Applicants with a remedy for the violation found. It would be absurd to require the Applicants to have had resort to a domestic remedy in the certain knowledge that such a claim would have failed.

CONCLUSION

89. The issues in this Application are of importance to many people across the whole of the Council of Europe. The Applicants respectfully ask the Court now to require the Government to provide its case with a measure of expedition, as explained in paragraph 4 (above).

2 March 2015

HELEN MOUNTFIELD QC
Matrix Chambers

TOM HICKMAN
RAVI MEHTA
Blackstone Chambers

ADAM HUNDT
DANIEL CAREY

Solicitors to the Applicants
Deighton Pierce Glynn Solicitors
Centre Gate
Colston Avenue
Bristol BS1 4TR

Tel: 0117 317 8133
Fax: 0117 317 8093
www.deightonpierceglynn.co.uk