IN THE INVESTIGATORY POWERS TRIBUNAL

B E T W E E N:

PRIVACY INTERNATIONAL

Claimant

-and-

(1) SECRETARY OF STATE FOR FOREIGN AND COMMONWEALTH AFFAIRS

(2) SECRETARY OF STATE FOR THE HOME DEPARTMENT

(3) GOVERNMENT COMMUNICATIONS HEADQUARTERS

(4) SECURITY SERVICE

(5) SECRET INTELLIGENCE SERVICE

Respondents

AMENDED STATEMENT OF GROUNDS

INTRODUCTION

1. Privacy International is a UK charity. It focuses, in particular, on ensuring that surveillance and the collection and use of data is carried out within the law, and providing protection for the right to privacy.

2. The Secretary of State for Foreign and Commonwealth Affairs is the minister responsible for oversight of the Government Communication Headquarters ("GCHQ") and the Secret Intelligence Service ("SIS"). The Secretary of State for the Home Department is the minister responsible for the Security Service. Together, GCHQ, SIS and the Security Service are referred to below as "the Agencies".

3. These proceedings concern the Agencies' acquisition, use, retention, disclosure, storage and deletion of Bulk Personal Datasets and the use of section 94 of the Telecommunications Act 1984.

4. These grounds accompany the forms T1 and T2 filed by the Claimant and set out the grounds relied upon. The Claimant will make written submissions and serve evidence in due course, once the Respondents have clarified the nature of their activities and their justification for them.

BULK PERSONAL DATASETS

5. On 12 March 2015, the Intelligence and Security Committee published its report "*Privacy and Security: A modern and accountable legal framework*" ("the ISC Report"). The ISC report disclosed, for the first time, the existence of Bulk Personal Datasets:

> "284. The publication of this Report is an important first step in bringing the Agencies 'out of the shadows'. It has set out in detail the full range of the Agencies' intrusive capabilities, as well as the internal policy arrangements that regulate their use. It has also, for the first time, avowed Bulk Personal Datasets as an Agency capability" (underlining indicates emphasis added).

The ISC concluded: "*BBB... the time has come for much greater openness and transparency regarding the Agencies' work*".

6. The ISC gave the following explanation of Bulk Personal Datasets:

a. Bulk Personal Datasets are "*large databases containing personal information about a wide range of people*" (p. 55).

b. Bulk Personal Datasets are used to identify subjects of interest, establish links between individuals and groups and improve understanding of a target's behaviour and connections, and to verify information obtained from other sources (p. 55).

c. The collection and search of Bulk Personal Datasets "*may be highly intrusive and impacts upon large numbers of people*" (p. 59Y).

d. Bulk Personal Datasets are "*an increasingly important investigative tool*" (§153).

e. Bulk Personal Datasets may be acquired through overt or covert means (§154).

f. Means of acquisition include where a person discloses data pursuant to section 19 of the Counter Terrorism Act 2008. As the Director General of the Security Service put it in evidence to the ISC "*in 2008, the Government deliberately… added section 19 of the Counter Terrorism Act, which is an explicit licensing to those who might share data, that doing so overrides any other duties of confidentiality which they might have about data, where a case is made that it is necessary to share that for national security*" (fn 138).

g. Bulk Personal Datasets vary in size "*from hundreds to millions of records*" and may be "*linked together so that analysts can quickly find all the information linked to a selector (e.g. a telephone number or a ***) from one search query*" (§156).

h. Bulk Personal Datasets affect British citizens ("*may include significant quantities of information about British citizens*" and "*none of the Agencies was able to provide statistics about the volume of personal information about British citizens that was included in these datasets*") (§158 and fn 142).

i. There has been minimal oversight and no clear legal regime governing the use of Bulk Personal Datasets:

   i. "*… the rules governing the use of Bulk Personal Datasets are not defined in legislation"* (§157).

   ii. The ISC "*has a number of concerns*" about the lack of a proper legal regime for the collection and use of Bulk Personal Datasets. In particular:

      1. Excessive and unjustified secrecy: "*…until publication of this Report, the capacity was not publicly acknowledged, and there had been no public or parliamentary consideration of the related privacy considerations and safeguards*".

      2. No legislative rules, restrictions or penalties for misuse: "*The legislation does not set out any restrictions on the acquisition, storage, retention, sharing and destruction of Bulk Personal Datasets, and no legal penalties exist for misuse of this information."*

      3. No system of warrants, or ministerial approval: "*Access to the datasets… is authorised internally within the Agencies without Ministerial approval*" and "*Ministers are not required to authorise the acquisition or use of Bulk Personal Datasets in any way…"* (§158, 159), although Ministers are "*often, but not always*" consulted before acquisition of a new dataset (but not the use of the dataset) (§159).

iii. There was no formal statutory oversight of the use of Bulk Personal Datasets (§160). That defect was only rectified on the day that the ISC Report was published (see below).

j. There has been abuse of Bulk Personal Datasets by the staff of all of the three Agencies. Each of the three Agencies "*had disciplined – or in some cases dismissed – staff for inappropriately accessing personal information held in these datasets in recent years*". As with any large aggregation of data about innocent people that can be accessed without a warrant, abuse is inevitable. No prosecutions appear to have been brought as a result of this unlawful conduct. Nor is it clear whether the victims of the conduct were notified so they could take appropriate steps to minimise the harm caused to them by the wrongful access to their information.

k. The Agencies have some internal procedures governing training and audits. Further, there "*may*" be additional controls around access to information about "*religion, racial or ethnic origin, political views, medical condition, ***, sexual orientation, or any legally privileged, journalistic or otherwise confidential information*" (§163). None of those procedures have been published, even in a gisted or redacted form.

l. Entire Bulk Personal Datasets may be given to foreign intelligence agencies. Not even the minimal safeguards described above apply where datasets are so shared ("… *while these controls apply within the Agencies, they do not apply to overseas partners with whom the Agencies may share the datasets*") (§163).

7. On the same day as the ISC Report was published, the Prime Minister signed the Intelligence Services Commissioner (Additional Review Functions) (Bulk Personal Datasets) Direction 2015. The Direction places the review of Bulk Personal Datasets by the Intelligence Services Commissioner onto a statutory basis.

8. Bulk Personal Datasets were defined in the Direction as follows:

> "5. For the purposes of this direct, a bulk personal dataset means any collection of data which:
>
> a. Comprises personal data as defined by section 1(1) of the Data Protection Act 1998;

b. Relates to a wide range of individuals, the majority of whom are unlikely to be of intelligence interest;

c. Is held, or acquired for the purposes of holding, on one or more analytical systems within the Security and Intelligence Agencies."

Therefore, the acquisition, retention and use of Bulk Personal Datasets involves keeping information on databases about large numbers of entirely suspicionless people who are of no legitimate intelligence interest.

9. The nature, scope and content of all of the Bulk Personal Datasets kept by the Agencies have been redacted from the ISC Report. However, the Bulk Personal Datasets are likely to include a variety of information, some volunteered, some stolen, some bought and some obtained by bribery or coercion:

a. **Retained telephony and internet communications data**: Telecommunications companies retained telephone and internet communications data, as required previously under the Data Retention Directive and now under the Data Retention and Investigatory Powers Act 2014. Such records include subscriber information, location, and length of phone calls. Internet communications data include billing records, and IP addresses.

b. **Data brokers and credit reference agencies**: Companies exist to harvest, trade or sell personal information, often for targeted advertising or to provide credit references. Credit reference agencies in the UK such as Experian, Equifax or Callcredit hold personal details on most of the adult population. These databases contain information such as loan borrowing and repayments, water and energy bills, payday loans, court records and fraud allegations. Some even include the direction of your garden (useful information for firms that sell solar panels or satellite dishes), whether you have a burglar alarm fitted, the make and mileage of your car, how much you spend on wine, sports and vitamins, if you gamble, where you go on holiday and what you read[1]. Information held by other databrokers includes lists containing

[1] http://www.thisismoney.co.uk/money/cardsloans/article-2324451/Credit-spies-making-millions-watching-move.html

sensitive personal information, such the identities of people with alcohol, sexual or gambling addictions.[2]

c. **Communication Service Providers**: As part of their businesses, communication service providers create large databases of their customers' private information. These can include a wide variety of content, such as chat logs, search histories and the content of emails.

Formatted: Justified

d. **Medical records**: Databases such as those held by the NHS Prescription Pricing Division hold all prescriptions written in England in the last five years. The NHS Personal Demographics Service, the national electronic database of NHS patients, could be acquired. The British Pregnancy Advisory Service, which is Britain's largest single abortion provider, holds hundreds of thousands of records for the 65,000 women they help each year. Private health records from BUPA or Nuffield Health will exist on a similar scale.

e. **Travel records**: Many databases contain detailed personal travel records. Oyster card transactions provide a detailed map of movements throughout London and similar databases could be obtained for other cities. Hotel reservation services, airline computerized reservation systems, as well as automatic number plate recognition databases, car rental databases from companies like Sixt, Europcar, or Enterprise, all contain personal information on a large number of people that may be of interest to the Agencies.

f. **Financial records**: Financial records from banks, transactional records from credit and debit cards provided by Visa or Mastercard; and interbank transaction databases such as SWIFT provide a detailed look at millions of peoples' lives.

g. **Biometric records**: Private companies such as AncestryDNA[3] hold more than 850,000 DNA records. Voiceprint records that identify who is speaking on the phone, or in a voice recording are held by companies such as ValidSoft. Facial recognition databases such as those created by face.com (now owned by Facebook) holds 18 billion face IDs.

[2] http://paramountdirectmarketing.com/
[3] http://dna.ancestry.co.uk/

h. **Membership databases**: Most membership bodies hold records in databases about their supporters, subscribers, or members. These could include databases held by political parties, professional associations, or religious databases belonging to churches, synagogues or mosques.

i. **Loyalty Card Schemes**: Many businesses offer loyalty cards, tracking consumers' buying habits in a way that can reveal extremely personal details, such as whether the buyer is pregnant. Tesco Clubcard has over 15 million members. Nectar Card has 19 million cardholders.

SECTION 94 OF THE TELECOMMUNICATIONS ACT 1984

10. Section 94 of the Telecommunications Act 1984 permits the Secretary of State to give national security directions to OFCOM and to providers of public electronic communications networks. Section 94 (as amended) provides:

> *(1) The Secretary of State may, after consultation with a person to whom this section applies, give to that person such directions of a general character as appear to the Secretary of State to be necessary in the interests of national security or relations with the government of a country or territory outside the United Kingdom.*
>
> *(2) If it appears to the Secretary of State to be necessary to do so in the interests of national security or relations with the government of a country or territory outside the United Kingdom, he may, after consultation with a person to whom this section applies, give to that person a direction requiring him (according to the circumstances of the case) to do, or not to do, a particular thing specified in the direction.*
>
> *(2A) The Secretary of State shall not give a direction under subsection (1) or (2) unless he believes that the conduct required by the direction is proportionate to what is sought to be achieved by that conduct.*
>
> *(3) A person to whom this section applies shall give effect to any direction given to him by the Secretary of State under this section notwithstanding any other duty imposed on him by or under Part 1 or Chapter 1 of Part 2 of the Communications Act 2003 and, in the case of a direction to a provider of a public electronic communications network, notwithstanding that it relates to him in a capacity other than as the provider of such a network.*
>
> *(4) The Secretary of State shall lay before each House of Parliament a copy of every direction given under this section unless he is of opinion that disclosure of the direction is against the interests of national security or relations with the government of a country or territory outside the United Kingdom, or the commercial interests of any person.*

Formatted: Font: Italic

Formatted: Indent: Left: 2.54 cm, Line spacing: single, No bullets or numbering

Formatted: Font: Italic

(5) A person shall not disclose, or be required by virtue of any enactment or otherwise to disclose, anything done by virtue of this section if the Secretary of State has notified him that the Secretary of State is of the opinion that disclosure of that thing is against the interests of national security or relations with the government of a country or territory outside the United Kingdom, or the commercial interests of some other person.

(6) The Secretary of State may, with the approval of the Treasury, make grants to providers of public electronic communications networks for the purpose of defraying or contributing towards any losses they may sustain by reason of compliance with the directions given under this section.

(7) There shall be paid out of money provided by Parliament any sums required by the Secretary of State for making grants under this section.

(8) This section applies to OFCOM and to providers of public electronic communications networks.

11. No section 94 direction has ever been laid before Parliament. All have been kept secret.

12. Section 94 is very broadly worded. It has recently been reported that section 94 has been used to require telecommunications companies to provide bulk access to communications data outside the protections of the RIPA regime (Gordon Corera *Intercept: The Secret History of Computers and Spies* (2105) p. 332.

13. It is therefore clear that:

a. Section 94 is potentially a means by which wide-ranging intrusions into privacy may occur.

b. There is no meaningful or effective oversight regime. In particular:

i. there is no statutory review by the Commissioner;

ii. there is no any provision for review of directions;

iii. there is no Code of Practice;

iv. there is no judicial authorisation; and

v. directions do not expire.

14. As with Bulk Personal Datasets, the use of section 94 has until recently been kept secret.

Formatted

Formatted

Formatted: Light Grid - Accent 4, Left, Right: 0 cm, Space After: 0 pt, Line spacing: single, No bullets or numbering, Hyphenate, Tab stops: Not at 1 cm

15. All public comments by independent reviewers have been critical. David Anderson QC in *A Question of Trust* said:

> 6.17 … s94… is very broad in nature and imposes no limit the kinds of direction that may be given. There is nothing in the public domain concerning the use of that power and the exercise of the s94 power is not subject to any oversight or external supervision.

> 13.31 … Obscure laws – and there are few more impenetrable than RIPA and its satellites – corrode democracy itself, because neither the public to whom they apply, nor even the legislators who debate and amend them, fully understand what they mean. Thus… TA 1984 s94… are so baldly stated as to tell the citizen little about how they are liable to be used.

16. The Interception of Communications Commissioner agreed to provide non-statutory oversight from March 2015 onwards over the (a) necessity and proportionality of section 94 directions; (b) the use of section 94; and (c) the safeguards for the use of section 94. The Commissioner explained that this work would not be able to begin immediately "*I will therefore require extra staff (and possibly technical facilities) to be able to carry out this oversight properly*" (IOCCO Report, March 2015, §10.4).

17. In July 2015, the Commissioner indicated that oversight had not yet started, and would not begin until "*the last quarter of 2015*" (§4.3). The Commissioner explained the serious problems encountered to date in his non-statutory oversight function:

> There are, however, some considerable challenges in this regard. The challenges stem from the fact that the directions are secret as followed for by statute, can be given by *any* Secretary of State and do not automatically expire after a certain period. There does not appear to be a comprehensive central record of the directions that have been issued by the various Secretaries of State. My office is therefore not yet in a position to be able to say confidently that we have been notified of all directions (italics in original).

18. The Commissioner also explained the limited nature of the oversight to date:

> 4.7 My office previously provided *limited* non-statutory oversight of the use made of one particular set of section 94 directions. This oversight was limited because it was only concerned with parts of c) above [i.e. safeguards]. My office was, and still is, prohibited from saying any more about this oversight as the Secretary of State is of the opinion that disclosure would be against the interests set out in section 94(5) of the Telecommunications Act.
>
> 4.8 My successor will hopefully be able to provide some further information in the next report about the progress of this oversight regime. I would echo the sentiments of others with regard to the avowal of any

Formatted: Font: Not Italic, No underline

Formatted: Font: Not Italic, No underline

Formatted: Indent: Left: 2.54 cm, Line spacing: single, No bullets or numbering

Formatted: Font: Italic

Formatted: Font: Italic

Formatted: Indent: Left: 2.54 cm, Line spacing: single, No bullets or numbering

Formatted: Indent: Left: 2.54 cm, Line spacing: single, No bullets or numbering

capabilities and the consolidation of relevant legislation to enable such matters to be debated and considered properly (italics in original).

LEGAL FRAMEWORK

Human Rights Act 1998 and European Convention of Human Rights

~~10.~~19. By section 6 of the Human Rights Act 1998, it is unlawful for a public authority to act in a way which is incompatible with one of the rights set out in Schedule 1 to the Act, which incorporates the European Convention on Human Rights ("ECHR").

~~11.~~20. Article 8 of the Convention provides:

> 1. *Everyone has the right to respect for his private and family life, his home and his correspondence.*
>
> 2. *There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.*

~~12.~~21. There are therefore four questions in any analysis of whether those rights have been breached:

a. Is the relevant right engaged?

b. Does the interference comply with the requirement of legal certainty imposed by the relevant Article?

c. Is the interference in pursuit of a legitimate aim?

d. Is the interference proportionate to the goal that is sought to be achieved (in the case of Article 8, "*necessary in a democratic society…*")?

Engagement of rights

~~13.~~22. Article 8 of the ECHR is clearly engaged in the present case. The acquisition, retention and use of a large database of information or the use of a national security direction to accumulate or intercept personal data plainly amounts to a serious interference

with the Article 8 right of privacy. See the judgment of the Grand Chamber of the CJEU in Case C-293/12 *Digital Rights Ireland* at §§33-34 and the judgment of the Grand Chamber of the ECHR in *S & Marper v UK* (2008) at §§70-86.

Legal certainty

~~14.~~23. Any interference with Article 8 must be "*in accordance with the law*" (see Article 8(2)). This requires more than merely that the interference be lawful as a matter of English law: it must also be "*compatible with the rule of law*": *Gillan v United Kingdom* (2010) 50 EHRR 45 at §76. There must be "*a measure of legal protection against arbitrary interferences by public authorities*", and public rules must indicate "*with sufficient clarity*" the scope of any discretion conferred and the manner of its exercise: *Gillan* at §77.

~~15.~~24. Numerous cases have addressed this requirement in the context of secret surveillance and information gathering.

a. In *Malone v United Kingdom* (1985) 7 EHRR 14, the Court held that the legal regime governing interception of communications "*must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to this secret and potentially dangerous interference with the right to respect for private life and correspondence*" §67. It must be clear "*what elements of the powers to intercept are incorporated in legal rules and what elements remain within the discretion of the executive*" and the law must indicate "*with reasonable clarity the scope and manner of exercise of the relevant discretion conferred on the public authorities*" §79.

b. In *Association for European Integration and Human Rights v Bulgaria* (62540/00, 28 June 2007), the Court held at §75:

> "*In view of the risk of abuse intrinsic to any system of secret surveillance, such measures must be based on a law that is particularly precise. It is essential to have clear, detailed rules on the subject, especially as the technology available for us is continually becoming more sophisticated […]*".

c. These requirements apply not only to the collection of material, but also to its treatment after it has been obtained, including the "*procedure to be followed for*

selecting for examination, sharing, storing and destroying intercepted material" (Liberty v UK (2009) 48 EHRR 1 at §69).

d. In Weber the ECHR held at §§93-94:

> "*The domestic law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures … Moreover, since the implementation in practice of measures of secret surveillance of communications is not open to scrutiny by the individuals concerned or the public at large, it would be contrary to the rule of law for the legal discretion granted to the executive or to a judge to be expressed in terms of an unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference."*

e. The Court continued in Weber by setting out at §95 the matters which any legal regime governing secret surveillance must expressly address in statute in order to be regarded as lawful:

> *"In its case law on secret measures of surveillance, the Court has developed the following minimum safeguards that should be set out in statute law in order to avoid abuses of power: the nature of the offences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or the tapes destroyed."*

~~16.~~25. The issue is whether the legal framework in fact contains adequate safeguards. It is no answer to assert that individual retention or use decisions made under the legal framework *could* be compatible with human rights. See the judgment of Lord Reed in R (T) v Chief Constable of Greater Manchester [2014] UKSC 35, [2014] 3 WLR 96 at §114:

> *"Determination of whether the collection and use by the state of personal data was necessary in a particular case involves an assessment of the relevancy and sufficiency of the reasons given by the national authorities. In making that assessment, in a context where the aim pursued is likely to be the protection of national security or public safety, or the prevention of disorder or crime, the court allows a margin of appreciation to the national authorities, recognising that they are often in the best position to determine the necessity for the interference. As I have explained, the court's focus tends to be on whether there were adequate safeguards against abuse, since the existence of such safeguards should ensure that the national authorities have addressed the issue of the necessity for the interference in a manner which is capable of satisfying the requirements of the Convention. In other words, in order for the interference to be "in accordance with*

the law", there must be safeguards which have the effect of enabling the proportionality of the interference to be adequately examined. Whether the interference in a given case was in fact proportionate is a separate question."[4]

~~17.~~26. Lord Reed also emphasised at §115 that whether a provision is "*in accordance with the law*" is not a matter on which a court should give deference to the decision maker:

> *"Whether a system provides adequate safeguards against arbitrary treatment, and is therefore "in accordance with the law" within the meaning of the Convention, is not a question of proportionality, and is therefore not a matter in relation to which the court allows national authorities a margin of appreciation."*

~~18.~~27. The Defendant's practice has been to keep the existence and identity of the Bulk Personal Datasets and the contents of section 94 directions entirely secret. Further, all access, oversight and regulation of the use of Bulk Personal Datasets occurs entirely in secret. Further, to date there has been no oversight or regulation of section 94 directions.

~~19.~~28. In circumstances where powers are exercised in secret, the case law of the ECHR stresses the importance of adequate safeguards. As the ECtHR has held: "*especially where a power of the executive is exercised in secret, the risks of arbitrariness are evident.*"[5] It is not sufficient that a power is *capable* of being exercised proportionately. What the national legislation must do is publicly to ensure that there are sufficient binding rules as to prevent arbitrary use of the power, and ensure that sufficient mandatory safeguards are in place to ensure that a power *is* exercised proportionately.

~~20.~~29. The case law of the ECtHR is clear that the minimum safeguards that should be set out in law in order to avoid abuses of power include a definition of the categories of people liable to have their data recorded and retained; a limit on the duration of the retention; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which the data may or must be erased. See *Malone v UK* (1985) 7 EHRR 14 at §68; *Liberty v UK* (2008) 48 EHRR 1 at §§62-69; and *Gillan v UK*

[4] Lord Wilson appeared to take a different approach to Lord Reed, but insofar as their judgments differed the remaining Justices indicated that they agreed with Lord Reed: see §158.

[5] *Malone v UK* (1985) 7 EHRR 14 at §67; *Huvig v France* (1990) 12 EHRR 528 at §29; *Rotaru v Romania* (App No 28341/95, 4 May 2000) at §55.

(2010) 50 EHRR 45 at §77. In *S and Marper v United Kingdom* (2009) 48 EHRR 50, the Court stated at §99:

> "*[The Court] reiterates that it is as essential, in this context, as in telephone tapping, secret surveillance and covert intelligence-gathering, to have clear, detailed rules governing the scope and application of measures, as well as minimum safeguards concerning, inter alia, duration, storage, usage, access of third parties, procedures for preserving the integrity and confidentiality of data and procedures for its destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness.*"

Legitimate aim and proportionality

~~21.~~30. The Claimant accepts that, in principle, data may be retained and used for legitimate aims such as national security. But there are no safeguards sufficient to limit the Defendants' retention and use of Bulk Personal Datasets solely for the purpose of national security.

~~22.~~31. Further, as set out below, the Claimant denies that the interference involved in the Agencies' acquisition and use of Bulk Personal Datasets, free from any material safeguards or constraints, constitutes a proportionate means of achieving a legitimate aim.

Claimant's standing

~~23.~~32. In order to pursue this complaint, the Claimant need not show that it has actually been the subject of the alleged interference. In the equivalent context of monitoring of communications, the European Court of Human Rights has held in *Liberty v United Kingdom* (2009) 48 EHRR 1 at §56 that:

> "*the mere existence of legislation which allows a system for the secret monitoring of communications entails a threat of surveillance for all those to whom the legislation may be applied. This threat necessarily strikes at freedom of communication between users of the telecommunications services and thereby amounts in itself to an interference with the exercise of the applicants' rights under art.8, irrespective of any measures actually taken against them*".

The same principles apply to this case.

33. Further, it is likely that information about the Claimant, and those that work for it, has been acquired using section 94 and is present in at least one Bulk Personal Dataset, given the potential breadth and scope of such databases.

EU law

Formatted: No bullets or numbering

34. Articles 7 of the Charter of Fundamental Rights of the EU provides:

> Everyone has the right to respect for his or her private and family life, home and communications.

Formatted: Indent: Left: 2.54 cm, Line spacing: single, No bullets or numbering

35. Article 8 provides an additional data protection right:

> 1. Everyone has the right to the protection of personal data concerning him or her.
>
> 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
>
> 3. Compliance with these rules shall be subject to control by an independent authority.

Formatted: Indent: Left: 2.54 cm, Line spacing: single, No bullets or numbering

36. Section 94 is within the scope of EU law and therefore subject to the Charter:

a. Article 5 of the e-Privacy Directive (2002/58/EC) requires that the confidentiality of telecommunications be ensured *except* when access is legally authorised in accordance with Article 15(1). This permits legislation to restrict the scope of the rights otherwise protected by the Directive "*when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. state security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC* [the Data Retention Directive]. *To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in the paragraph.*"

Formatted

Formatted: Font: Italic

Formatted: Font: Italic

b. Article 15(1) of the e-Privacy Directive authorised Member States to adopt domestic legislation to restrict the rights and obligations:

> "Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use or the

Formatted: Indent: Left: 3.49 cm, Line spacing: single, No bullets or numbering

electronic communications system, as referred to in Article 13(1) of Directive 95/46/EC. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union."

c. A national measure that imposes intercept or retention requirements on a commercial telecommunications provider is therefore within the scope of EU law, and must comply with the requirements of Article 15(1) of the e-Privacy Directive. See the judgment of the Grand Chamber of the CJEU in *Digital Rights Ireland* [2015] QB 127 and of the Divisional Court in *R (Davis & Watson) v SSHD* [2015] EWHC 2092 (Admin).

Formatted

37. EU law under Articles 7 and 8 of the Charter requires (in addition to the Strasbourg case law) that access to personal data be subject to prior review by a court or other independent body, and that there be proper protection for privileged materials.

Domestic legal regime governing the relevant conduct

~~24.~~38. As the ISC noted, the domestic legal regime governing Bulk Personal Datasets is extremely sparse.

~~25.~~39. The collection of Bulk Personal Datasets appears to be often carried out under section 19 of the Counter Terrorism Act 2008. Section 19 provides:

> *"(1) A person may disclose information to any of the intelligence services for the purposes of the exercise by that service of any of its functions.*
>
> *(2) Information obtained by any of the intelligence services in connection with the exercise of any of its functions may be used by that service in connection with the exercise of any of its other functions.*
>
> *(3) Information obtained by the Security Service for the purposes of any of its functions may be disclosed by it –*
>
> *(a) for the purpose of the proper discharge of its functions,*
>
> *(b) for the purpose of the prevention or detection of serious crime, or*
>
> *~~(c)~~© for the purpose of any criminal proceedings.*
>
> *(4) Information obtained by the Secret Intelligence Service for the purposes of any of its functions may be disclosed by it –*

(a) for the purpose of the proper discharge of its functions,

(b) in the interests of national securit~~y,~~

©(c) for the purpose of the prevention or detection of serious crime, or

(d) for the purpose of any criminal proceedings.

(5) Information obtained by GCHQ for the purposes of any of its functions may be disclosed by it –

(a) for the purpose of the proper discharge of its functions, or

(b) for the purpose of any criminal proceedings.

(6) A disclosure under this section does not breach –

(a) any obligation of confidence owed by the person making the disclosure, or

(b) any other restriction on the disclosure of information (however imposed)."

~~26.~~40. Receipt or disclosure of information pursuant to Section 19 of the 2008 Act does not require any warrant or other external authorisation, regardless of the private or sensitive nature of the information concerned.

~~27.~~41. Other powers may also be used to collect information for storage in a Bulk Personal Dataset, such as:

a. the warrant regime governing intercept in RIPA;

b. sections 5 or 7 of the Intelligence Services Act 1994; or

c. section 94(1) of the Telecommunications Act 1984 which permits the Secretary of State to make a direction to a communication service provider, including a direction to provide access to data.

~~28.~~42. In general terms, for all public and private bodies the retention and processing of personal data is governed by the Data Protection Act 1998 ("the DPA"). However, the Agencies enjoy an extremely wide exemption from the DPA where a national security certificate has been made under section 28 of the DPA. For example, GCHQ's certificate provides for the following exemption:

PART A			
	Column 1		Column 2
1.	Personal data processed in the performance of the functions described in section 3 of the Intelligence Services Act 1994 ("ISA") or personal data processed in accordance with section 4(2)(a) ISA.	i) ii) iii) iv) v)	Sections 7(1),10 and 12 of Part II; Sections 16(c), 16(e), 16(f),17,21,22 and 24 of Part III; Part V; the first data protection principle; the second data protection principle;
2.	Personal data relating to the vetting of candidates, staff, contractors, agents and other contacts of GCHQ in accordance with the Government's security and vetting guidelines and policy including but not limited to:	vi) vii)	the sixth data protection principle to the extent necessary to be consistent with the exemptions contained in this certificate; and the eighth data protection principle.

29.43. The Data Protection Principles are as follows. The principles in **bold type** are abrogated by the Certificate:

> **"1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless—**
>
> > **(a) at least one of the conditions in Schedule 2 is met, and**
> >
> > **(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.**
>
> **2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.**
>
> 3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
>
> 4. Personal data shall be accurate and, where necessary, kept up to date.
>
> 5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
>
> **6. Personal data shall be processed in accordance with the rights of data subjects under this Act.**
>
> 7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
>
> **8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data."**

30.44. The effect of the Certificate is thus that:

a. Personal data need not be processed fairly or lawfully and the conditions in Schedule 2 (or for sensitive personal data, Schedule 3) need not be complied with (Principle 1).

b. Personal data can be collected or obtained for one purpose but used for another.

c. There are no restrictions on the transfer of data outside the EEA, even where the recipient will not provide an adequate level of protection for the data.

~~31.~~45. Further, no warrant is required to obtain, access or process data. Data can thus be freely obtained from agents or by data gathering operations not involving interception of communications and thereafter retained. For example, the Respondents could encourage (or pay or bribe) an agent to give access to:

a. all the emails or messages sent and received (including content as well as communications data) of users of a large internet service provider; or

b. all of the medical records of patients held on a database

and hold all of that information in a Bulk Personal Dataset.

GROUNDS

~~32.~~46. The regime governing the acquisition, use, retention, disclosure, storage and deletion of Bulk Personal Datasets is not sufficiently accessible to the public, nor does it contain adequate safeguards to provide proper protection against arbitrary conduct. The context is that Bulk Personal Datasets contain information, which may be extremely intrusive and sensitive, about very large numbers of people, the majority of whom are of no legitimate intelligence interest whatsoever:

a. No warrant (whether judicial or otherwise) is required to obtain a Bulk Personal Dataset, regardless of the sensitivity of the data obtained, or the size and scale of the dataset. Further, Bulk Personal Datasets are linked together to allow automated federated searching across multiple databases, thus increasing the intrusiveness of the searches. For example, if an employee of an internet email provider offered (or perhaps was bribed) to give the Agencies access to its database of emails, such information could be accepted and

utilised as a Bulk Personal Dataset without needing to obtain any authorisation or warrant. The same would apply to a database of all computerised medical records held by GPs and hospitals in London. Further, all of the safeguards and limitations on bulk intercept (such as those in section 16 of RIPA) would be circumvented or avoided.

b. Access, use or processing of any Bulk Personal Dataset may be carried out without any warrant (or section 16 RIPA certificate), even if the same information (if still held by the originator thereof) would normally require a warrant providing for property interference or intercept.

c. There are no temporal limits on the acquisition or retention of data. In contrast, a warrant only has a limited period of validity.

d. There is no Code of Practice or other public set of rules or policies governing the acquisition, use, retention, disclosure, storage and deletion of Bulk Personal Datasets.

e. There are no restrictions on the transfer of Bulk Personal Datasets to other intelligence agencies outside the UK, even where the recipient will not provide adequate protection or safeguards for the security or use of the dataset. No safeguards apply where datasets are shared. Further, there are no publicly available rules governing the transfer of such Bulk Personal Datasets.

f. Until the publication of the ISC's report, there was no statutory provision for the oversight of Bulk Personal Datasets by the Intelligence Services Commissioner.

g. Until the publication of the ISC's report, the capacity to hold and use Bulk Personal Datasets was not publicly acknowledged, and there was no public or parliamentary consideration of the necessary privacy considerations and safeguards. As a result, there are no such public safeguards. Such secrecy was excessive and unjustified and did not serve any proper national security purpose, as the publication of information in the ISC report has shown.

h. The inadequacy of the rules and procedures governing Bulk Personal Datasets is shown by the fact that each Agency has encountered cases of

misuse of the datasets. Nor do there appear to have been any criminal prosecutions for such misuse.

i. There is no procedure to notify victims of any misuse of a Bulk Personal Dataset, so that they can seek an appropriate remedy before the Tribunal.

47. The regime governing the acquisition, use, retention, disclosure, storage and deletion of private information under section 94 is not sufficiently accessible to the public, nor does it contain adequate safeguards to provide proper protection against arbitrary conduct:

a. The general words of section 94 could be used to circumvent the limitations and safeguards applicable to interception and acquisition of communications data set out in RIPA.

b. There is no provision for the review of directions.

c. No central or accessible record has been maintained of the section 94 directions made by the various Secretaries of State.

d. Section 94 directions do not expire, and are not limited in time. In contrast, a warrant only has a limited period of validity, as required by *Weber*.

e. Until March 2015, there was no independent oversight of section 94 directions. From March 2015, the oversight has been non-statutory and has not yet commenced.

f. There is no Code of Practice or other public set of rules or policies governing the acquisition, use, retention, disclosure, storage and deletion of personal data under section 94.

g. There is no requirement for judicial authorisation.

48. Further, and in any event, any retention of the Claimant's details on a Bulk Personal Dataset, or using section 94 is not necessary or proportionate.

Formatted

Formatted

~~33.~~49. In the premises, the regime governing Bulk Personal Datasets and directions under section 94 was and remains contrary to Article 8 ECHR, Articles 7 and 8 of the Charter and Article 15(1) of the e-Privacy Directive.

CONCLUSION

~~34.~~50. The Claimant therefore seeks the following orders:

a. A declaration that the Respondents' use of Bulk Personal Datasets is unlawful;

b. A declaration that the regime for giving directions under section 94 of the Telecommunications Act 1984 is unlawful;

c. An order for the quashing of any section 94 directions currently in force;

~~a.~~d. An order disapplying section 94;

~~b.~~e. An order requiring the destruction of any unlawfully obtained material;

f. An injunction restraining further unlawful conduct;~~.~~

~~c.~~g. Such further or other relief as the Tribunal thinks fit.

THOMAS DE LA MARE QC

BEN JAFFEY

THOMAS DE LA MARE QC

BEN JAFFEY

10 September 2015