Case No. IPT/15/110/CH

IN THE INVESTIGATORY POWERS TRIBUNAL

B E T W E E N:

PRIVACY INTERNATIONAL

Claimant

-and-

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

Respondents

WITNESS STATEMENT OF SAM SMITH

I, Sam Smith, Coordinator at MedConfidential, Lambert Place, Lewes BN7 2EL **SAY AS FOLLOWS:**

Introduction

1. medConfidential is an independent non-partisan organisation founded in 2013 working for confidentiality and consent in health and social care. I joined medConfidential in 2013 after 2 years at Privacy International.

2. All staff members at medConfidential have given evidence to Parliament's Health Select Committee[1] on issues around medical records. In 2014, I was appointed to the National Information Board of the Department of Health[2], and in 2015 I was invited to join the Privacy and Consumer Advisory Group of the

[1] http://www.parliament.uk/business/committees/committees-a-z/commons-select/health-committee/inquiries/parliament-2010/cdd-2014/

[2] https://www.gov.uk/government/organisations/national-information-board

8. The Information Commissioner's Office submissions on the draft Investigatory Powers Bill refers to 'substantial policy reasons'[6] why such data (medical records) should not be available in bulk. The ICO said:

> There is increasing centralisation of records such as with the Care.data program and other effort to create significant national level collections of health related information.[7]

9. The ICO asked for medical records to be exempted from Bulk Personal Datasets.

Background

Personal Data

10. The Data Protection Act 1998 states in Part I Preliminary:

> "Personal data means data which relate to a living individual who can be identified –
> (a) from those data, or
> (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,
> and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

11. The Information Commissioner states:

> It is important to note that, where the ability to identify an individual depends partly on the data held and partly on other information (not necessarily data), the data held will still be "personal data".[8]

---

[6] Paragraph 33 Joint Committee on the Draft IPB ICO submission https://ico.org.uk/media/about-the-ico/consultation-responses/2016/1560392/draft-investigatory-powers-bill-the-information-commissioners-submission.pdf [accessed on 3 May 2016]

[7] Paragraph 33 Joint Committee on the Draft IPB ICO submission https://ico.org.uk/media/about-the-ico/consultation-responses/2016/1560392/draft-investigatory-powers-bill-the-information-commissioners-submission.pdf [accessed on 3 May 2016]

[8] https://ico.org.uk/for-organisations/guide-to-data-protection/key-definitions/ [accessed on 3 May 2016]

12. GCHQ's Guidance for completing the BPD form October 2012 to June 2014[9] states on page 1 of 4 claims that anonymized data is not a Bulk Personal Dataset:

> This guide provides instructions for completing the Bulk Personal Data Acquisition and Retention form. The BPDAR process is an internal policy authorisation used to authorise acquisition and/or retention of operational data by GCHQ, where the data is: Bulk in nature (i.e. not narrowly focused on a particular target), and Personal (i.e. deals with individuals and contains real names).
>
> (footnote: GCHQ agreed with Cabinet Office in 2010, as part of the Review of Agency Handling of Bulk Personal Data, that, to be considered personal data, a dataset has to contain at least the actual names of individuals.)

The NHS Number

13. "Everyone registered with the NHS in England, Wales and the Isle of Man has a unique patient identifier called NHS Number."[10] "An NHS number is used across all NHS organisations and is the only national unique single data item to identify and connect your health records."[11]

14. Since commencement of the Health and Social Care (Safety and Quality) Act 2015[12] on 1 October 2015,[13] it has been a legal requirement for medical records to include the NHS number to allow for unique identification of individuals. Prior to that date, while it was not a legal requirement, it was the norm for NHS numbers to be used for individuals by most organisations, and use has has been widespread since the current form of the NHS number was introduced in 1996.

15. As such, the NHS number provides a unique identifier, which can either be used as a selector, or which can be used to match databases.

16. Such databases include the creation of the national "Hospital Episode Statistics - Secondary Uses Service" (HES - SUS) datasets, where most (if

---

[9] Document '3)' from Documents dating from June 2005 to May 2014 disclosed pursuant to paragraph 5 of the order of 15 January 2016

[10] http://www.nhs.uk/NHSEngland/thenhs/records/nhs-number/Pages/what-is-the-nhs-number.aspx

[11] http://systems.hscic.gov.uk/nhsnumber/patients/faqs

[12]

[12] http://www.nhs.uk/chq/Pages/1889.aspx?CategoryID=68

not all) hospital and other care is amalgamated at a national level. That dataset may not include a patient's name, but will include the NHS number.

The Contents of Medical Records

17. A medical record is a linked, lifetime, detailed, comprehensive record of medical or social care events, both physical and mental, for each person in the UK.

18. According to the NHS website:[14]

> "A health record (sometimes referred to as medical record) should contain all the clinical information about the care you received. This is important so every healthcare professional involved at different stages of your care has access to your medical history, such as allergies, operations or tests. Based on this information, healthcare professionals can make judgments about your care going forward.
>
> Your health records should include everything to do with your care, including x-rays or discharge notes. The data in your records can include:
>
> - treatments received or ongoing
> - information about allergies
> - your medicines
> - any reactions to medications in the past
> - any known long-term conditions, such as diabetes or asthma
> - medical test results such as blood tests, allergy tests and other screenings
> - any clinically relevant lifestyle information, such as smoking, alcohol or weight
> - personal data, such as your age, name and address
> - consultation notes, which your doctor takes during an appointment
> - hospital admission records, including the reason you were admitted to hospital
> - hospital discharge records, which will include the results of treatment and whether any follow-up appointments or care are required
> - X-rays
> - photographs and image slides, such as magnetic resonance imaging (MRI) or computerised tomography (CT) scans"

14

19. The official Department of Health "guidance on keeping health records"[15] for General Practice says:

> "Electronic patient records must not be destroyed or deleted for the foreseeable future."

20. According to the NHS:

> "Wherever you visit an NHS service in England a record is created for you. This means medical information about you can be held in various places, including your GP practice, any hospital where you've had treatment, your dentist practice, and so on.
>
> At times, this can delay information sharing which can affect decision making and slow down treatment."

21. The NHS number, and the increase in use of electronic patient records, is designed to increase the speed and ease of that information sharing.

22. Using data linkage from the NHS number, the Health and Social Care Information Centre maintains a repository called the Secondary Uses Service.

23. "The Secondary Uses Service (SUS) is the single, comprehensive repository for healthcare data in England which enables a range of reporting and analyses to support the NHS in the delivery of healthcare services."[16]

24. When records are used for purposes beyond direct care, such as in the Secondary Uses Service, they are "de-identified" which means names are removed but the NHS number can remain, and is heavily used in national consolidated datasets:[17]

> "In April 2010, the NHS Operations Board agreed that the NHS number should normally form part of the datasets submitted for contractual payments under the NHS standard contract.
>
> ...
>
> Many commissioners and providers already use NHS Numbers as part of the payment process to identify patients. The data used by commissioners may be provided locally or as part of a national data set submitted to the Secondary Uses Service (SUS).

---

[15] http://www.nhs.uk/chq/Pages/1889.aspx?CategoryID=68&SubCategoryID=160
[16] http://www.hscic.gov.uk/sus
[17] http://systems.hscic.gov.uk/nhsnumber/staff/commissioning

... The NHS Operating Framework 2012/13 states;
3.29 No single technical change has greater power to improve the integration of services than the consistent use of the NHS number. NHS organisations are expected to use the NHS number consistently in 2012/13 and commissioners should link the use of the NHS number to contractual payments in line with the guidance. There will be punitive contract sanctions for any organisation not compliant by 31 March 2013."

25. Until early 2015, SUS was delivered under contract by BT Global Services, which describes SUS as "one of the largest enterprise data warehouses in the world. It is in the top three per cent by size and number of users across all industries. Currently running to 67 Terabytes of data".[18]

26. In terms of record count "the SUS holds around 10 billion pseudonymised records."

Medical confidentiality

27. In the language of the medical profession, data and privacy are discussed in the frame of "confidentiality".

28. The British Medical Association "Confidentiality and disclosure of health information Toolkit" introduces "General Information"[19] on "The Duty of Confidentiality" as:

> "Confidentiality is an essential requirement for the preservation of trust between patients and health professionals and is subject to legal and ethical safeguards. Patients should be able to expect that information about their health which they give in confidence will be kept confidential unless there is a compelling reason why it should not. There is also a strong public interest in maintaining confidentiality so that individuals will be encouraged to seek appropriate treatment and share information relevant to it."[20]

---

[18] http://www.globalservices.bt.com/uk/en/casestudy/nhs_sus
[19] Card 2, BMA confidentiality toolkit http://www.bma.org.uk/-/media/files/pdfs/practical%20advice%20at %20work/ethics/confidentialitytoolkit_card2.pdf
[20] Page 44, BMA confidentiality toolkit.

29. In short, if patients believe that their medical records will not be confidential, they may not disclose information that is necessary to a correct diagnosis or the correct medical care.

30. The right to confidentiality is not absolute. The BMA continues:[21]

> "any decision as to whether identifiable information is to be shared with third parties must be made on a case by case basis and must be justifiable in the 'public interest'"

31. Where a lawful authority makes a request for an individual's medical records, there is a process to be followed, which protects every party in the public interest:

> "Disclosures in the public interest based on the common law are made where disclosure is essential to prevent a serious and imminent threat to public health, national security, the life of the individual or a third party or to prevent or detect serious crime."

32. The BMA also notes that, "Ultimately, the public interest can only be determined by the courts."[22]

33. Any use of medical records as a bulk personal dataset is fundamentally incompatible with a case by case basis decision.

34. Speaking at the Investigatory Powers Bill Committee of the House of Commons on 26th April, Home Office Minister John Hayes said:[23]

> *"I am prepared in this specific instance to confirm that the security and intelligence agencies do not hold a bulk personal dataset of medical records. Furthermore, I cannot currently conceive of a situation where, for example, obtaining all NHS records would be either necessary or proportionate.*

35. As welcome as that statement is, it does not speak to past practices, or subsets of "NHS records". Nor does state whether any non-UK database has been obtained.

---

[21] Page 44, BMA confidentiality toolkit.
[22] Page 44, BMA confidentiality toolkit.
[23] Column 549, Investigatory Powers Bill Committee, House of Commons. 2015. http://www.publications.parliament.uk/pa/cm201516/cmpublic/InvestigatoryPowers/160426/pm/PBC_Investigatory%20Powers%2012th%20sit%20(pm)_26_04_2016.pdf

Social Care

36. Speaking in the same debate, Sir Keir Starmer QC MP discussed the impact of bulk personal datasets on social care:[24]

> "I will take an example from child social care. A child may be reporting and having recorded some of the most grotesque offences that have happened to them, in an environment where it is hoped that the right relationship will be built up through the process of child social care—in other circumstances, adult social care—so that they obtain the best care possible. Persuading people into that sort of relationship, so that they can get the support they need, is not easy, as anyone who has experience in this area will know.
>
> ...
>
> "Getting children to engage with child social care is the devil's own business in many difficult cases. There are many reasons why children do not engage. If children, vulnerable adults and those with mental health problems cannot see clear protection on the face of the Bill that applies to them—not in a flexible way—it would be a retrograde step in relation to all the good work going on in other parts of the forest on offences such as child sexual exploitation.

37. Those receiving social care are amongst the most vulnerable in society, often with complex conditions and a variety of concerns. It is both the appearance of actions, as well as actions themselves, that are critical to the broader public policy, beyond the narrow remit of the Secretary of State for the Home Department.

Scope - Sensitive data

38. I have read the Respondents' disclosure, and the definitions they draw. There are a number of references to medical records and contradictory information within and between the agencies about whether medical records constitute 'sensitive data' and thus attract different safeguards on the same information.

39. Document RFI 34, page 4, defines various relevant terms under the heading "DETAILS OF CATEGORIES OF PERSONAL DATA THAT SIS DEEMS TO BE PARTICULARLY INTRUSIVE":

---

[24] Column 548.

Disability/Medical Condition

The definition in law for sensitive personal data includes "physical or mental health or condition".
This is information about a condition itself, as opposed to confidential information shared with a doctor (see below). In addition to medical conditions, this category includes blood group; physical characteristics (hair/eye colour); and biometrics (iris/fingerprint scans etc)
[redacted]

...

Medical Info
This refers only to information that would be confidential between a doctor and their patient.

40. For domestic consideration, as regards the contents of medical records:[25]

> *"It is recognised that the degree of interference with an individual's rights and freedoms may be higher where the communication data being sought relates to a person who is a member of a profession that handles privileged or otherwise confidential information (including medical doctors, lawyers, journalists, Members of Parliament or ministers of religion known as `sensitive professions`"*

41. Reading the Sensitive Profession Definitions, RFI 30, it is very clear:

> Medical doctors
> These exclude dentists, physiotherapists, nurses or mental health professionals.

42. This would appear to exclude, for example, a Chartered Clinical Psychologist will have extremely sensitive conversations with a patient, but is excluded from protection under this policy.

Circumstances

43. Interception of communications may only take place prospectively; whereas data is almost exclusively retrospective. In the case of medical records, it is

[25] RFI 29; red box: "Designated Persons - Implementing the new Code of Practice for Privileged Communications Data"

since birth, and through linkage to the NHS records of the mother, also prenatal care. Every life event, even as a child, is permanently recorded until death, and then for posterity afterwards.

Alternatives

44. There are alternative mechanisms by which medical records can be overtly acquired from the clinicians who act as data controllers. If medical records are required as part of an investigation by the Agencies, those mechanisms ought to be used.

45. The General Medical Council states[26]:

Disclosure without consent

Occasionally, there will be circumstances where you have to disclose a patient's records without their consent (and, rarely, in the face of the patient's clear objection to disclosure). There are three possible justifications for this:

• If you believe that a patient may be a victim of neglect or abuse, and that they lack capacity to consent to disclosure, you must give information promptly to an appropriate person or authority, if you believe disclosure is in the patient's best interests.

• You believe that it is in the wider public interest, or that it is necessary to protect the patient or someone else from the risk of death or serious harm. Examples of this might be to inform the DVLA if someone may be unfit to drive, or to assist the police in preventing or solving a serious crime, or informing the police if you have good reason to believe that a patient is a threat to others. You should follow GMC guidance (Confidentiality) on disclosure within the wider public interest.

• Disclosure is required by law – for example, in accordance with a statutory obligation, or to comply with a court order or a disclosure notice from the NHS Counter-Fraud Service.

Care.data

[26] http://www.gmc-uk.org/guidance/ethical_guidance/confidentiality.asp

46. Since 1989, the NHS has been collecting data on hospital stays, known as hospital episode statistics (HES).

47. In the late summer of 2013, NHS England attempted to launch its care.data programme using posters and leaflets in GP surgeries. Whilst some patients may have opted out, the Information Commissioner intervened and determined that the communications and method did not meet fair processing requirements.

48. The aim of Care.data is to expand the database to include what happens to patients when they are under the care of GPs. The Care.data service will upload all GP patient records in England to a central database, to be used for medical research by both the NHS and private companies such as pharmaceutical firms. A similar service already exists for hospital records, but this is the first time it has been extended to basic GP records.[27]

49. The majority of people visit their GPs more frequently than hospital and GPs will generally have someone's lifetime of conditions, prescriptions, family history, blood tests and referrals. It is a rich dataset.

50. In January 2014 NHS England sent out an unaddressed leaflet to households across England. Some people received or read a copy of the leaflet, others did not.

51. Despite widespread criticism of the poor public awareness campaign, and reports that only 1 in 9 people received the leaftlet, nevertheless hundreds of thousands of people went to the internet of their own accord, downloaded forms for themselves and/or family members, printed them off and filled them in, ticking two boxes, and either posted them back to their GP practice or delivered them in person. The Health and Social Care Information Centre estimated as of 11 June 2015 that '700,000'[28] people did so.

52. This level of public response demonstrates the concern of the public in respect of use of their data. Having to go online and download forms is a relatively high barrier to entry. The response highlights levels of concern.

---

[27] http://www.computerweekly.com/blogs/editors-blog/2014/02/the-lesson-from-the-nhs-careda.html

[28] Letter to the Health Select Committee from the Chair of HSCIC http://data.parliament.uk/writtenevidence/ committeeevidence.svc/evidencedocument/health-committee/handling-of-nhs-patient-data/written/18661.pdf

53. According to a Pulse survey[29] over 40% of GPs intended to opt themselves out of care.data scheme. Pulse stated:

> A substantial number of GPs are so uneasy about NHS England's plans to share patient data that they intend to opt their own records out of the care.data scheme, reveals a Pulse snapshot survey.
>
> The survey of nearly 400 GP respondents conducted this week found the profession split over whether to support the care.data scheme, with 41% saying they intend to opt-out, 43% saying they would not opt-out and 16% undecided.[30]

54. A further survey by Pulse reported that two thirds of the public did not recall receiving the care.data information leaflet.[31]

55. On 20 April 2016 the Information Commissioner's Office made a public statement on Health and Social Care Information Centre stating:

> An undertaking to comply with the Data Protection Act 1998 has been signed by Health and Social Care Information Centre (HSCIC)[32]. The ICO has found that patients were offered an opportunity to opt out from their data being shared with other organisations, but that the opt outs were not implemented. HSCIC have agreed a series of steps to remedy this. The undertaking explains the background and the reasons for delays in reaching this point.
>
> Steve Eckersley, Head of Enforcement at the ICO, said:
>
> "People were given the choice to opt out of having their medical data shared in this way, and would have expected their decision to be respected. It was not. While we note the reasons for the delays around this, patients' data has been processed unfairly and we have taken action to put that right."

Data losses

---

[29] http://www.pulsetoday.co.uk/your-practice/practice-topics/it/over-40-of-gps-intend-to-opt-themselves-out-of-caredata-scheme/20005648.article [accessed on 3 May 2016)

[30] http://www.pulsetoday.co.uk/your-practice/practice-topics/it/over-40-of-gps-intend-to-opt-themselves-out-of-caredata-scheme/20005648.article [accessed on 3 May 2016)

[31] http://www.pulsetoday.co.uk/your-practice/practice-topics/it/two-thirds-of-public-dont-recall-receiving-caredata-information-leaflet/20005874.fullarticle

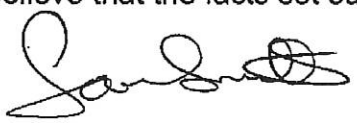
[32] https://ico.org.uk/media/action-weve-taken/undertakings/1623957/hscic-undertaking-20160419.pdf
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/517835/20april16chairsaction.pdf

56. The NHS are required to report even small losses of data. The same requirements do not apply to other medical bodies. Big Brother Watch has reported on NHS Data Breaches. Their November 2014 Report[33] states in Key Findings that:

> All results are for the years 2011 to 2014 unless otherwise indicated.
> A full list of NHS organisations is available in tables 2-7.1
> • There have been at least 7,255 breaches. This is equivalent to: o 2,418 breaches every year. o 201 breaches every month. o 46 breaches every week. o6 breaches every day.
> • There have been:
> o At least 50 instances of data being posted on social media
> o At least 143 instances of data being accessed for "personal reasons"
> o At least 124 instances of cases relating to IT systems
> o At least 103 instances of data loss or theft
> o At least 236 instances of data being shared inappropriately via Email, letter or Fax o At least 251 instances of data being inappropriately shared with a third party
> o There were 115 cases of staff accessing their own records.
>
> • There have been at least 61 resignations during the course of disciplinary proceedings.
>
> • There is 1 court case pending, for a breach of the Data Protection Act. In this instance the individual may have also resigned prior to proceedings.

STATEMENT OF TRUTH

I believe that the facts set out in this witness statement are true.



Sam Smith

3 May 2016

[33] https://www.bigbrotherwatch.org.uk/wp-content/uploads/2014/11/EMBARGO-0001-FRIDAY-14-NOVEMBER-BBW-NHS-Data-Breaches-Report.pdf

Case No. IPT/15/110/CH

IN THE INVESTIGATORY POWERS TRIBUNAL

B E T W E E N:

PRIVACY INTERNATIONAL

Claimant

-and-

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

Respondents

WITNESS STATEMENT OF CAMILLA GRAHAM WOOD

I Camilla Graham Wood, Legal Officer of Privacy International, 62 Britton Street, London, EC1M 5UY SAY AS FOLLOWS:

1. I am a qualified solicitor admitted to the roll of solicitors in England and Wales on 3 October 2011. I have worked at Privacy International since December 2015 as Legal Officer and I am authorized to make this statement on behalf of Privacy International.

2. Prior to my employment at Privacy International I worked at Birnberg Peirce and Partners.

3. In 2014 I was awarded the Law Society Junior Lawyer Excellence Award and Legal Aid Practitioners Group Young Legal Aid Lawyer of the Year.

4. The contents of this statement are based on identified sources.

Bulk Personal Datasets

5. Bulk Personal Datasets are "large databases containing personal information about a wide range of people"[1].

6. 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 revealed for the first time the existence of Bulk Personal Datasets held by the Agencies. It said:

[1] http://isc.independent.gov.uk/news-archive/12march2015 [accessed on 3 May 2016] page 55

> 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.[2]
>
> *Other intrusive capabilities*
>
> xiv. We have also examined a number of other intrusive capabilities that are used by the Agencies (paragraphs 151–193). These include both the explicit capabilities defined in RIPA (such as the use of surveillance and the use of agents), and those capabilities that are implicitly authorised through general provisions in the Security Service Act 1989 and the Intelligence Services Act 1994 (such as the use of IT Operations against targets overseas and the acquisition of Bulk Personal Datasets). Our Report contains a number of detailed recommendations, primarily in relation to: greater transparency, to the extent that this is possible without damaging national security; and specific statutory oversight by either the Intelligence Services Commissioner or the Interception of Communications Commissioner in those areas where oversight is currently undertaken on a non-statutory basis.[3]

7. The ISC Report also said that "the rules governing the use of Bulk Personal Datasets are not defined in legislation."[4]

8. The report went on to state that Bulk Personal Datasets are large databases containing personal information about a wide range of people, which are used in three ways[5]:

> '1. To help identify SoIs or unknown individuals who surface in the course of investigations;
> 2. To establish links between individuals and groups or elsewhere improve understanding of a target's behavior and connections; and
> 3. As a means of verifying information that was obtained through other sources (such as agents).

9. The Report goes on to state that SIS explained that Bulk Personal Datasets:

> *'…are increasingly used to identify the people that we believe that we have an interest in; and also to identify the linkages between those individuals and the UK that we might be able to exploit.***.*[6]

10. Whilst considerable amounts of the Report is redacted, the Report gives an impression of a targeted or limited approach in relation to use of Bulk Personal Datasets. This is undermined by what has been revealed in the disclosure received in the course of these proceedings, together with the Respondents' Closed Response and Closed Response to Request for Further Information. As set out below, the breadth of information obtained as

---

[2] http://isc.independent.gov.uk/news-archive/12march2015 [accessed on 3 May 2016] page 108 - 109

[3] http://isc.independent.gov.uk/news-archive/12march2015 [accessed on 3 May 2016] page 6

[4] http://isc.independent.gov.uk/news-archive/12march2015 [accessed on 3 May 2016] page 56

[5] http://isc.independent.gov.uk/news-archive/12march2015 [accessed on 3 May 2016] page 55

[6] http://isc.independent.gov.uk/news-archive/12march2015 [accessed on 3 May 2016] page 55 citing Oral Evidence – SIS 15 May 2014

part of Bulk Personal Datasets is expansive, untargeted and goes beyond use in investigations, establishing links and verifying information.

11. The ISC Report indicated the volume of information held by the Intelligence Agencies in Bulk Personal Datasets saying:

> 156. These datasets vary in size from hundreds to millions of records. Where possible, Bulk Personal Datasets may be linked together so that analysts can quickly and all the information linked to a selector (e.g. a telephone number or ***) from one search query. *** [7]

12. The ISC Report noted that none of the agencies was able to provide statistics about the volume of personal information about British Citizens included in the datasets. It reported that:

> 158...
>
> - Access to the datasets – which may include significant quantities of personal information about British Citizens – is authorized internally within the Agencies without Ministerial approval.[8]
>
> Footnote 142: None of the Agencies was able to provide statistics about the volume of personal information about British Citizens that was included in these datasets.[9]
>
> 163...
> The Agencies may use stronger controls around access to certain sensitive information. Depending on the context, this may include, but is not limited to, personal information such as an individual's religion, racial or ethnic origin, political views, medical condition, ***, sexual orientation, or any legally privileged, journalistic or otherwise confidential information.[10]

13. The ISC Report also raised concerns regarding the lack of independent authorisation and lack of restrictions on acquisition, storage, retention, sharing and destruction:

> 158. The Committee has a number of concerns in this respect:
>
> - Until the publication of this Report, the capability was not publicly acknowledged, and there had been no public or Parliamentary consideration of the related privacy considerations and safeguards.
> - 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.

---

[7] http://isc.independent.gov.uk/news-archive/12march2015 [accessed on 3 May 2016] page 56 citing Written Evidence – SIS 5 March 2014

[8] http://isc.independent.gov.uk/news-archive/12march2015 [accessed on 3 May 2016] page 57

[9] http://isc.independent.gov.uk/news-archive/12march2015 [accessed on 3 May 2016] page 57

[10] http://isc.independent.gov.uk/news-archive/12march2015 [accessed on 3 May 2016] page 58

- Access to the datasets – which may include significant quantities of personal information about British citizens – is authorised internally within the Agencies without Ministerial approval.[11]

14. Additional concerns in respect of acquisition include:

> 159. While Ministers are not required to authorise the acquisition or use of Bulk Personal Datasets in any way, the Home Secretary explained that she had some involvement: '[MI5] *do come to me and I receive submissions on acquisition of bulk datasets and the holding of bulk datasets*". In relation to the Bulk Personal Datasets held by GCHQ and SIS, the Foreign Secretary explained to the Committee that: *"There's not a formal process by which we've looked* [at those datasets]". However, this is an area which he is currently reviewing. He explained:[12]
>
> > [I am] *often, but not always, consulted before acquisition of new datasets... I was consulted recently on a specific acquisition of a dataset that has been made. Following that, I asked for a report from SIS, which I've had, about their holdings and the handling arrangements, following which I asked to make a visit for a discussion about this and an understanding of how it works in practice... I have also asked for twice yearly reporting of the holdings of bulk personal data by the agencies.*[13]

15. Following the ISC Report, little further information about bulk personal datasets was revealed until the publication of the draft Investigatory Powers Bill[14] ("IPB").

Draft IPB evidence 2015 / 2016[15]

16. The Draft Investigatory Powers Bill was published in November 2015. A Joint Committee[16] was formed to examine the Bill. Evidence was submitted from a wide range of organisations.

17. David Anderson QC the Independent Reviewer of Terrorism Legislation[17], said in oral evidence to the Committee:

> "I welcome this Bill, Lord Chairman. The law in this area has, until now, provided for extensive but vague powers, used in a way that the citizen could not predict and safeguarded by people who, for all their very considerable merits, have not been particularly visible to Parliament or the public. I would single out two major improvements that have already been happening over the 18 months since I started doing my review, A Question of Trust, though there is no causal relationship there, of course.

---

[11] http://isc.independent.gov.uk/news-archive/12march2015 [accessed on 3 May 2016] page 57
[12] http://isc.independent.gov.uk/news-archive/12march2015 [accessed on 3 May 2016] page 57
[13] Oral Evidence – Foreign Secretary, 16 October 2014
[14] http://www.publications.parliament.uk/pa/jt201516/jtselect/jtinvpowers/93/93.pdf accessed on 3 May 2016
[15] http://www.parliament.uk/draft-investigatory-powers [accessed on 3 May 2016]
[16] http://www.parliament.uk/draft-investigatory-powers
[17] https://terrorismlegislationreviewer.independent.gov.uk

The first is the disclosure of significant and sometimes controversial powers that are already used but that people did not really know about before. You are looking there at bulk collection, the use of bulk personal datasets, the practice of equipment interference or hacking by the Government, and very recently, indeed on the morning the Bill was launched, a very significant data retention power that was previously almost entirely unknown. Many of those disclosures were prompted by proceedings in the Investigatory Powers Tribunal.

If you are looking at accessible and foreseeable, it seems to me that it is not just about the Bill; it is about getting more material into the public domain as to the utility of some of these powers, in particular bulk, which sits there like an elephant in the room. We have heard discussions about how one can look to see if someone's wife is using the car and whether that is collateral intrusion and so on, but if you are tapping a cable that potentially gives you access to the conversations of thousands or hundreds of thousands of people, you are looking at some very major issues. [18]

18. In oral evidence on 07.12.15 Professor Mark Ryan[19], Professor of Computer Security, University of Birmingham said in relation to bulk provisions that:

"because they allow for the collection and automatic processing of data about people who are not suspected of any crime…I do not think it is correct to say that this is not a recipe for mass surveillance. It is the processing of data about everybody, and in my opinion that is mass surveillance."[20]

19. Lord Strasburger, a member of the Joint Committee, said that:

"The Bill and Explanatory notes are very vague about BPD and the ISC report was vague and hugely redacted. The Home Office will not tell the Committee the identity of the databases it is scooping up, so it is very difficult for the Joint Committee to assess the proportionality, risks and intrusiveness of the collection of BPD."[21]

Theresa May evidence to Joint Committee

On 13 January 2016 Theresa May gave evidence to the Joint Committee.

20. Lord Strasburger asked questions regarding Bulk Personal Datasets and indicated specific concerns about medical records:

---

[18] http://www.parliament.uk/documents/joint-committees/draft-investigatory-powers-bill/oral-evidence-draft-investigatory-powers-committee.pdf Oral Evidence Taken Before the Joint Committee on Wednesday 2 December 2015 Question 61

[19] https://www.cs.bham.ac.uk/~mdr/ [accessed on 3 May 2016]

[20] http://www.parliament.uk/documents/joint-committees/draft-investigatory-powers-bill/oral-evidence-draft-investigatory-powers-committee.pdf Oral Evidence Taken Before the Joint Committee on Monday 7 December 2015 Question 86

[21] http://www.parliament.uk/documents/joint-committees/draft-investigatory-powers-bill/oral-evidence-draft-investigatory-powers-committee.pdf Oral Evidence Taken Before the Joint Committee on Monday 7 December 2015 Question 92

Q272 Lord Strasburger: Turning to bulk personal datasets, the lack of clarity about them has been a concern for many witnesses and Committee members. We understand that there are databases that exist in the public and private sectors and that each contains personal information about potentially millions of innocent citizens. We also understand that the security intelligence agencies have for some time been getting copies of this data, either with or without the owner's permission, and once again without the explicit approval of Parliament for them to do so. Some witnesses have told us that these datasets have been medical records, bank account data and other highly personal information. In order to establish the truth about bulk personal datasets, the Committee has asked the Home Office many times for a list of them, which has been refused on every occasion. My question is: how can the Committee form a view on the appropriateness of the secret ingestion of bulk personal datasets without having any idea what they are?[22]

....

Lord Strasburger: It is not possible to exclude certain datasets like medical records.

Theresa May MP: No. As soon as you start excluding certain datasets, that gives messages to those who would seek to do us harm about the way in which the authorities operate.[23]

...

Disclosure regarding history of BPD

21. There has been no explanation from the Intelligence Agencies or the Government about the history of the acquisition, use and so forth of Bulk Personal Datasets. It is unclear when datasets became classified by each agency as 'Bulk Personal Datasets' as opposed to another categorization of datasets or simply 'Bulk Data'.

22. On 8 December 2001 the Foreign Secretary signed a section 28 Certificate in respect of GCHQ[24] and MI6[25]. The Home Secretary signed a section 28 Certificate in respect of MI5[26] on 10 December 2001. Those certificates remain in effect.

23. The historical documents dating from June 2005 to May 2014[27] refer sporadically to Bulk Personal Datasets. It appears that whilst what are now classified as 'Bulk Personal Datasets' were obtained prior to this period, they were not formally identified as such nor in a

[22] http://www.parliament.uk/documents/joint-committees/draft-investigatory-powers-bill/oral-evidence-draft-investigatory-powers-committee.pdf Oral Evidence Taken Before the Joint Committee on Wednesday 13 January 2016 Question 272

[23] http://www.parliament.uk/documents/joint-committees/draft-investigatory-powers-bill/oral-evidence-draft-investigatory-powers-committee.pdf Oral Evidence Taken Before the Joint Committee on Wednesday 13 January 2016 Question 272

[24] Respondents Documents enclosed with response to RFI [RFI 3]

[25] Respondents Documents enclosed with response to RFI [RFI 33]

[26] Respondents Documents enclosed with response to RFI [RFI 12]

[27] Respondents Documents dating from June 2005 – May 2014 disclosed pursuant to paragraph 5 of the Order of 15 January 2016

particular oversight regime. There were sporadic references to whether the bulk data contained personal information. It is not clear what happened if the relevant box was ticked on the form asking this question[28].

24. GCHQ Compliance Extracts 2010 to June 2014[29] refers to Bulk Personal Data once on page 2 of 15 stating in the 'Extracts from 'Analysis' section of the Compliance Guide April 2014 that:

> Communications about targets Bulk personal data
>
> GCHQ acquires and stores some data sets that contain a high proportion of information relating to individuals. This data is either acquired lawfully from GCHQ's own collection operations, or from other parties. In the latter case, acquisition is authorised and recorded by obtaining a Data Acquisition Authorisation (DAA). Some of these data sets are classed as targeted bulk personal data sets i.e. they are personal because each record contains at least the name of an individual, but there is something about the data that implies a reasonable expectation that much of it will contain information of intelligence value to GCHQ. Some of these data sets are classed as non-targeted bulk personal data sets i.e. they are personal because each record contains at least the name of an individual, but the majority of the data is not believed to relate to probable intelligence targets. The relevant policy team makes the decision about what is targeted and non-targeted bulk personal data, in consultation with data owners. The following types of data include both.

25. GCHQ's Guidance for completing the BPD form October 2012 to June 2014[30] states on page 1 of 4:

> This guide provides instructions for completing the Bulk Personal Data Acquisition and Retention form. The BPDAR process is an internal policy authorisation used to authorise acquisition and/or retention of operational data by GCHQ, where the data is: Bulk in nature (i.e. not narrowly focused on a particular target), and Personal (i.e. deals with individuals and contains real names).
>
> > (footnote: GCHQ agreed with Cabinet Office in 2010, as part of the Review of Agency Handling of Bulk Personal Data, that, to be considered personal data, a dataset has to contain at least the actual names of individuals.)

---

[28] For example: Historical Document 6B. Security Service Standard Forms for Acquisition v5 page 2; Historical Document 7A Security Service Standard Forms for Sharing v5, v5.1, v6, v6.2, v7.1 page 3; Historical Document 8A Security Service Standard Forms for Retention v5, v5.1, v6, v6.2, v7.1 page 2; Historical Document 22 Secret Intelligence Service Authorisation of Bulk Data Acquisition / Transformation Authorisation *[labelled on the index 'Authorisation of Bulk Personal Dataset' but the document is in fact headed 'Bulk Data Acquisition / Transformation Authorisation']*; Historical Document 23 Secret Intelligence 'Data Authorisation Form' *[labelled on the index 'Authorisation of Bulk Personal Dataset Form v2 March 2012 to December 2012' but the document is in fact headed 'Data Authorisation Form']*

[29] Document '2)' from Documents dating from June 2005 to May 2014 disclosed pursuant to paragraph 5 of the order of 15 January 2016

[30] Document '3)' from Documents dating from June 2005 to May 2014 disclosed pursuant to paragraph 5 of the order of 15 January 2016

The purposes of the BPDAR process are:

To account for GCHQ's acquisition and retention of bulk personal data, so that we can demonstrate to our oversight bodes that a suitably senior and experienced GCHQ officer has considered whether the acquisition and ongoing retention of the data is necessary and proportionate in relation to one or more of GCHQ's authorised purposes under the Intelligence Services Act, and To ensure that we have a better knowledge of what bulk personal data we hold and where it is stored.

This guidance should be read in conjunction with What is Bulk Personal Data?

26. There is no other mention of Bulk Personal Datasets in the GCHQ documents. The Security Service refers to 'personal data' in a 2006 document. 'Bulk External Data Acquisition Internal Authorisation Process 2006'[31]. It appears that up to this point Bulk Personal Datasets were acquired as part of Bulk Data Acquisition. The form asks on page 6 of 12:

> Please explain the level of intrusion into privacy: (Issues you should explore include - The nature of the data (it is personal data etc?) Does the database contain a high or low proportion of people of no intelligence interest? Is the data anonymous and will it remain so? [for example could other data or techniques available to the Service be used to remove this anonymity?] Have you requested the totality of the database or a subset and does this help to manage intrusion? Who in the Service will have access to the data?)

27. The Security Service 'Bulk External Data Authorisation – Internal Authorisation Process document dated 2006[32] indicates a large amount of confusion regarding Bulk Data in general and an attempt to classify bulk personal datasets on page 2 of 12:

> 'Key issues:
>
> - Outside of specialist areas, current bulk data request authorisation processes are unclear and not widely understood.
> - Bulk data requests are increasing and are often being made by desks unfamiliar with best practice.
> - This combination generates risks

28. The document refers to 'trial' of proposals on page 8 of 12 which appear to be the basis for BPDs. It states on page 2 of 12 that:

> 'The relevant team holds a list of data already in the Service. [REDACTED] However, although it is likely to be accurate I cannot guarantee that it provides a total capture of all bulk data in the Service as there are no comprehensive records.' It states that 'As there is no central authorisation policy it is not possible to validate that best practice has been followed in all data requests. Any policy that we do establish has to cope with: a) Other regimes for some data (e.g. RIPA) b) Confusion over what is meant by 'Bulk Data' c) Varying data sizes and sensitivities d) Low general awareness of guidance on issues to

[31] Document '4)' from Documents dating from June 2005 to May 2014 disclosed pursuant to paragraph 5 of the order of 15 January 2016

[32] Document '4)' from Documents dating from June 2005 to May 2014 disclosed pursuant to paragraph 5 of the order of 15 January 2016

consider when seeking bulk data.

29. The document proposes on page 3 of 12 that bulk data should be defined at 'a. Electronic data sets that are too large to be easily susceptible to manual b. processing and contain data about multiple individuals.'

30. In Version 5 of the Security Service Standard Forms for Acquisition[33] we see on page 1 of 6 it is asked whether data 'includes data about individuals of no intelligence interests that may be of personal or sensitive nature'. This indicates that personal and sensitive datasets were collected but not under the BPD regime, which appears not to have been in existence.

31. The Security Service 'Loose Minute' dated 31 March 2006[34] addressed to MI5 officials from MI5 officials, it refers on page 1 of 2 to initial guidance for 'The database'. It is not clear whether this is for either or both Bulk Personal Datasets and Bulk Communications Data as subsequent internal documents refer to BCDs.

32. The Secret Intelligence Service documents date back to 2009 and refer to bulk data acquisition and exploitation. Further information is provided in the 'User Comms 2011 – 2014' document[35] which includes abuse of the datasets. The document states that they have 'now' formalized Service policy on the acquisition, exploitation and retention of bulk data. At the end of the former document is states:

> 'However if it is likely that they may be of future use, data can be retained off the database in storage.'

33. The Respondents have not provided information regarding retention off the database.

34. The Secret Intelligence Service refer in November 2010 to using the database to exploit Bulk Personal Data.

Anonymity or not

35. The 'Open' version of the Respondents' Closed Response (undated), served on the Claimant on 11 April 2016 defined Bulk Personal Datasets as:
    1) A Bulk Personal Dataset ("BPD") is a dataset that contains personal data about individuals that majority of whom are unlikely to be of intelligence interest and that is incorporated into an analytical system and used for intelligence purposes.[36]
    ...
    3) BPD obtained and exploited by the Intelligence Services include a number of broad categories of data. By way of example only these include: biographical and travel (e.g.

[33] Document '6B)' from Documents dating from June 2005 to May 2014 disclosed pursuant to paragraph 5 of the order of 15 January 2016
[34] Document '9)' from Documents dating from June 2005 to May 2014 disclosed pursuant to paragraph 5 of the order of 15 January 2016
[35] Document '21)' from Documents dating from June 2005 to May 2014 disclosed pursuant to paragraph 5 of the order of 15 January 2016
[36] Page 1, paragraph A.1) of The Respondents Closed Response, open version

passport databases); communications (e.g. telephone directory); and financial (e.g. finance related activity of individuals).[37]

36. There is a lack of clarity regarding anonymity of Bulk Personal Datasets and what happens when data is integrated. Security Service Standard Forms for Acquisition v7[38] asks on page 7 of 8 'is the information contained in the dataset anonymous?'

37. The Security Service Loose Minute dated 31 March 2006[39] states on page 1 of 2:

> 'Anonymity – all data will remain anonymous until we choose to match the data to other material that will identify the telephone users or use RIPA to request subscriber information.'

38. However, documents[40] including GCHQ Guidance for completing the BPD form dated June 2014 to present[41], state 'GCHQ agreed with Cabinet Office in 2010 as part of the Review of Agency Handling of Bulk Personal Data, that to be considered personal data, a dataset has to contain at least actual names of individuals.'

Types of data acquired

39. For an increasing number of people, personal digital devices contain the most private information they store anywhere. Computers and mobile devices have replaced and consolidated our filing cabinets, photo albums, video archives, personal diaries and journals, address books, and correspondence. They are also slowly replacing our formal identification documents and our bank and credit cards. They hold information that may never have been set down or communicated elsewhere.

40. The Respondents Response states that sources of Bulk Personal Datasets include:

> '54. §4.2.1 notes the wide range of sources from which MI5 acquired BPD (such as SIA Partners, other HMG Departments, private business, interception and CNE). §4.2.2 sets out the broad categories of MI5's acquired datasets.

41. The documents thus indicate a number of methods by which Bulk Personal Datasets may be obtained by Computer Network Exploitation[42] and Covert Human Intelligence Sources[43] including user of covert methods by 'Supplier Organisation'[44]

---

[37] Pages 1-2, paragraph A.3`) of The Respondents Closed Response, open version

[38] Document '6C)' from Documents dating from June 2005 to May 2014 disclosed pursuant to paragraph 5 of the order of 15 January 2016

[39] Document '9)' from Documents dating from June 2005 to May 2014 disclosed pursuant to paragraph 5 of the order of 15 January 2016

[40] Page 1 of 4, RFI 3 of Documents Enclosed with Response to RFI;

[41] RFI 7 of Documents Enclosed with Response to RFI

[42] Respondents Closed Response to the Factual Allegations page 13 of 65;
Respondents Amended Open Response, page 15 of 47, paragraph 63;
RFI 4 of Documents Enclosed with Response to RFI: GCHQ Compliance Guide Extracts June 2014 to present. Pages 10 of 19, 11 of 19 and 17 of 19;
Document '8D)' from Documents dating from June 2005 to May 2014 disclosed pursuant to paragraph 5 of the order of 15 January 2016, page 2 of 5;

42. Documents state that if the information is obtained through commercial means then it is not Bulk Personal Dataset including Security Service Bulk External Data Acquisition Internal Authorisation Process 2006:

> c) Make plain that this policy does **not** apply to any data that is acquired commercially (eg.: [REDACTION])
> d) We do not seek to broaden this policy to cover all data held by the Service.[45]

RFI 16 of Documents Enclosed with Response to RFI: Security Service Bulk Personal Data Guidance November 2015 to present, page 5 of 20 and page 13 of 20;
RFI 20 of Documents Enclosed with Response to RFI: Security Service BPD Form for Retention current, page 2 of 6;
RFI 21 Security Service BPD Handling Arrangements for Bulk Personal Data November 2015 to present, page 6 of 14;
Exhibit B to Respondents Closed Response, MI5 Closed BPD Handling Arrangements November 2015 to present, page 6 of 14;
Exhibit G to Respondents Closed Response, Form for Retention (undated), page 2 of 6.

[43] Document '1)' from Documents dating from June 2005 to May 2014 disclosed pursuant to paragraph 5 of the order of 15 January 2016, page 2 of 5: GCHQ Compliance Guide Extracts page numbered 16;
Document '8E)' from Documents dating from June 2005 to May 2014 disclosed pursuant to paragraph 5 of the order of 15 January 2016: Security Service Standard Forms for Retention, page 2 of 5;
RFI 1 of Documents Enclosed with Response to RFI: All Intelligence Agencies, SIA Bulk Personal Data Policy, February 2015 page 11 of 14;
RFI 17 of Documents Enclosed with Response to RFI: Security Service BPD Policy November 2015, page 12 of 15;
RFI 20 of Documents Enclosed with Response to RFI: Security Service BPD Form for Retention. Current page 2 of 6;
RFI 21 of Documents Enclosed with Response to RFI: Security Service BPD Handling Arrangements for Bulk Personal Data November 2015, page 3 of 14;
RFI 46 of Documents Enclosed with Response to RFI: Secret Intelligence Service handling arrangements for Bulk Personal Data November 2015, page 3 of 14;
Exhibit A to Respondents Closed Response: SIA Bulk Personal Data policy February 2015 page 12 of 15;
Exhibit G to Respondents Closed Response: Form for Retention (undated) page 2 of 6.

[44] Document '8E)' from Documents dating from June 2005 to May 2014 disclosed pursuant to paragraph 5 of the order of 15 January 2016: Security Service Standard Forms for Retention, page 2 of 5;
RFI 16 Security Service Bulk Personal Data Guidance November 2015 to present, page 5 of 20 and 13 of 20;
RFI 20 Security Service Bulk Personal Data Form for Retention. Current. Page 2 of 6;
[45] Document '4)' from Documents dating from June 2005 to May 2014 disclosed pursuant to paragraph 5 of the order of 15 January 2016: Security Service Bulk External Data Acquisition Internal Authorisation Process 2006, page 3 of 12;

and the Security Service Policy for Bulk Data Acquisition Sharing Retention and Deletion October 2010 to March 2015:

> Finally, commercially and openly available datasets (e.g. GB Info, Companies House etc) and data generated by corporate systems is not bulk data. The handling of these datasets is not covered by this policy.
> ...
> The [Bulk Data Review] Panel weighs up each dataset's usage over the 6 month period against necessity, proportionality, level of intrusion and the potential corporate, legal, reputational and political risk. The Panel also considers the frequency of acquisition and updates and whether such information could be acquired elsewhere, by for example, commercial means...
> ...
> Has the data been provided by the individual to a non-government body (e.g. within the commercial sector)?
> [46]

43. The documents do nevertheless refer to 'BPD Categories' that include commercial data. The Security Service Bulk Personal Guidance March 2015 to November 2015 page 2 states:

> Definition of Data Categories
> BPD Categories
> MI5 currently categorises its BPD holdings into the following:
> ...
> Commercial: These datasets provide details of corporations/individuals involved in commercial activities.

44. In addition, the documents[47] also refer to commercial sources for Bulk Personal Data: 'Data Source: Likely to be mainly SIS, BSS, OGD or commercial providers. Could be GCHQ itself.'[48] and if it is attached to an email it also does not come under this regime.

---

[46] RFI 13 of Documents Enclosed with Response to RFI: Security Service Policy for Bulk Data Acquisition Sharing Retention and Deletion October 2010 to March 2015, page 2, 5 and 8

[47] RFI 4 of Documents Enclosed with Response to RFI: Compliance Guide Extracts June 2014 to present, page 4 of 20;
RFI 7 of Documents Enclosed with Response to RFI: GCHQ Guidance for completing the BPD Form June 2014 to present, page 2 of 8 and 6 of 8;
RFI 15 of Documents Enclosed with Response to RFI: Security Service Bulk Personal Data Guidance March 2015 to November 2015 page 9 of 12;
RFI 16 of Documents Enclosed with Response to RFI: Security Service Bulk Personal Data Guidance November 2015 to present;

Document '6B)' from Documents dating from June 2005 to May 2014 disclosed pursuant to paragraph 5 of the order of 15 January 2016: Security Service Standard Forms for Acquisition v5 page 1 of 6;
Document '6C)' from Documents dating from June 2005 to May 2014 disclosed pursuant to paragraph 5 of the order of 15 January 2016: Security Service Standard Forms for Acquisition v7 page 7 of 8;

45. It is noted that there is a potential indication of the use of covert means against Other Government Departments:

> Respondents' Response
> 19. We obtain some of our bulk datasets through Other Governmental Departments (OGNs) and other intelligence agencies (SIS and GCHQ). Each OGD has their own obligation to protect data that is provided to them, and the Service should consider this when reviewing shared datasets.
>
> 20. We may wish to retain the shared dataset longer than the OGD recommends. If the original data provider **is aware** that we hold their data, we may approach them directly to explain why we need to keep the data for longer. [REDACTION]

46. The ISC Report also mentioned covert action could be used to acquire BPDs.[49] At its simplest, covert collection could take the form of physical stealing of the data from a company. There are GCHQ HUMINT (human intelligence) Operations Teams[50] who are tasked with "identifying, recruiting and running covert agents". Another common tactic used is bribery, with recent news showing Drug Enforcement Agency paid employees of foreign telecommunications firms for copies of similar databases.[51]

47. The disclosure confirms that Bulk Personal Datasets contain communication content and refer to assessing the need to 'examine the content of communications', as stated for example in RFI 4 at page 1 of 20:

> It is your responsibility to make relevant analysts aware of any significant changes that may affect the legality of the targeting of selectors, or mean that additional authorisation is required to examine the content of communications...If you are examining the content of individuals' communications the standard of your HRA justification must be higher than if you are examining events data. No additional authorisation is needed for querying and examining events data.[52]

Exhibit H to Respondents Closed Response, MI5 policy for bulk data acquisition and deletion October 2010 (page 10 of 12);

[48] Document '3)' from Documents dating from June 2005 to May 2014 disclosed pursuant to paragraph 5 of the order of 15 January 2016: GCHQ Guidance for completing the BPD form October 2012 to June 2014 page 2 of 4;

[49] ISC report, page 56

[50] http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security

[51] ttp://www.usatoday.com/story/news/2015/04/07/dea-bulk-telephone-surveillance-operation/70808616/

[52] RFI 4 of Documents Enclosed with Response to RFI: Compliance Guide Extracts June 2014 to present pages 1 of 19, 2 of 19, 15 of 19, 19 of 19 ;

48. Datasets are likely to include a variety of information, some volunteered, some bought and some obtained through CHIS / interception and other sources. Datasets include:

- ***Population*** (these datasets provide population data or other information which could be used to help identify individuals e.g. passport details)[53]
- ***Travel*** (these datasets contain information which enable the identification of individuals' travel activity)[54]
- ***Finance*** (these datasets allow the identification of finance related activity of individuals)[55]
- ***Communications*** (these datasets allow the identification of individuals where the basis of information held is primarily related to communications data e.g. a telephone directory)[56]
- Other information held or obtained in relation to 'persons to whom he provides the service, by a person providing a Telecommunications service': Credit card details of bill payee, or the email address owner would fall within this category[57]
- Billing data and feasibility checks for all UK telephone numbers[58]
- Geo-location where the user is known to be located in the UK[59];
- GCHQ typically requests the following categories of communications data from CSP's:

  a. subscriber related information such as subscriber details for a given telecommunications address, lists of telecommunications addresses associated with a given premises, reverse name searches, tip-offs if telecommunications addresses reassigned to different subscribers, tip-offs if subscriber ports telecommunications address to a different CSP, etc.
  b. billing information[60]

- Authorisation for acquisition of bulk personal data form[61] asks if the following has been obtained:

---

[53] Intelligence Agencies closed response to the factual allegations
[54] Intelligence Agencies closed response to the factual allegations
[55] Intelligence Agencies closed response to the factual allegations
[56] Intelligence Agencies closed response to the factual allegations
[57] Document '1)' from Documents dating from June 2005 to May 2014 disclosed pursuant to paragraph 5 of the order of 15 January 2016: GCHQ Compliance Guide Extracts as at 1 June 2005 to 2010, labelled page 207
[58] Document '1)' from Documents dating from June 2005 to May 2014 disclosed pursuant to paragraph 5 of the order of 15 January 2016: GCHQ Compliance Guide Extracts as at 1 June 2005 to 2010, labelled page 211
[59] Document '1)' from Documents dating from June 2005 to May 2014 disclosed pursuant to paragraph 5 of the order of 15 January 2016: GCHQ Compliance Guide Extracts as at 1 June 2005 to 2010 labelled page 211
[60] Document '1)' from Documents dating from June 2005 to May 2014 disclosed pursuant to paragraph 5 of the order of 15 January 2016: GCHQ Compliance Guide Extracts as at 1 June 2005 to 2010, labelled page 208
[61] Document '3A)' from Documents dating from June 2005 to May 2014 disclosed pursuant to paragraph 5 of the order of 15 January 2016: Guidance for completing the BPD form (October 2012 to June 2014), page 2 of 8

Name; DOB; Nationality; Address; Telephone number(s); Email address; ID number; Passport details; Organisation / occupation; Banking / credit cards / other financial information; Travel details; Medical details; Religious information; Other

- Later forms include 'financial transaction details'[62] and 'Financial. This includes transactional data that allows you to understand the financial activity of an individual. It would also include obviously private data or a combination of information which would allow a person to leverage goods and services. [redacted].'[63]

- The Authorisation for acquisition of bulk personal data form[64] asks:
  Does the dataset contain a high proportion of data on people of no probable intelligence interest?
  Does it contain a significant proportion of data about UK nationals?
  Does it contain a significant proportion of data about foreign partner nationals
  Does it contain information about minors?

- Forms are required where a bulk dataset…[65]
  - Is likely to include large amounts of superfluous or non-targeted data
  - Includes data about individuals of no intelligence interest that may be of a personal or sensitive nature
  - Has been generated by any external organization or partner agency and exhibits the above characteristics

  Forms are not required where the bulk dataset…
  - Relates to a targeted individual or has been acquired under an existing oversight mechanism
  - Is considered open source and is therefore already in the public domain
  - Has been procured commercially
  - Has been generated from within the Security Service

  ...

  Does the database contain personal information
  - Identifying personal data
  - Information about activities (e.g. travel)
  - Sensitive personal data (financial, medical, religious, journalistic, political, legal)"

The Agencies consider information that should be treated as 'sensitive' for handling purposes and lists[66]:

- Biometric data
- Related to a Member of Parliament

---

[62] RFI 5 of Documents Enclosed with Response to RFI: GCHQ BDP FORM January 2016 to present, page 3 of 18;
[63] RFI 35 of Documents Enclosed with Response to RFI: Secret Intelligence Services Bulk Personal Data Guidance on the Authorisation Process December 2014 to October 2015, page 5
[64] Document '3A)' from Documents dating from June 2005 to May 2014 disclosed pursuant to paragraph 5 of the order of 15 January 2016: Guidance for completing the BPD form (October 2012 to June 2014), page 3 of 8
[65] Document '6B)' from Documents dating from June 2005 to May 2014 disclosed pursuant to paragraph 5 of the order of 15 January 2016: Standard Forms for Acquisition, v5-0, page 1 of 6
[66] RFI 1 of Documents Enclosed with Response to RFI: All Intelligence Services . SIA Bulk Personal Data Policy February 2015, page 3 of 14.

- About journalists
- Employment within the SIA
- Information that is operationally sensitive to the SIA
- Information subject to legal professional privilege.

Expanding upon the medical information collected the disclosure refers to:

- Dentists, physiotherapists, nurses or mental health professionals[67]
- Medical records[68]
- Disability/Medical condition: The definition in law of sensitive personal data includes 'physical or mental health or condition'. This is information about a condition itself, as opposed to confidential information shared with a doctor (see below). In addition to medical conditions this category includes blood group; physical characteristics (hair/eye colour); and biometrics (iris/fingerprint scans etc) [redacted].[69]
- Medical info: this refers only to information that would be confidential between a doctor and their patient.

49. Sir Kier Starmer QC MP told Parliament that:

> 'Although it was not formal evidence, the Committee had a briefing session with the security and intelligence services where the question arose whether they do in fact access health records. In those exchanges, the answer was, 'No we don't, at the moment'.'[70]

50. This statement does not clarify whether the intelligence agencies held such data in the past, or intend to do so in the future.

51. In the same Committee session John Hayes MP, representing the government stated that:

> 'I am prepared in this specific instance to confirm that the security and intelligence agencies do not hold a bulk personal dataset of medical records.'

52. This statement also fails to provide clarity in relation to medical records. As shown by the disclosure there are a number of different datasets and large databases that contain a variety of different material. This statements fails to clarify whether medical records, medical information, medical condition, health data or other related data is held in datasets and databases of the intelligence agencies in the past or at present.

Intrusiveness

---

[67] RFI 30 of Documents Enclosed with Response to RFI: Security Service. Section 94. Sensitive Professions Definitions April 2015 to present

[68] RFI 4 of Documents Enclosed with Response to RFI: GCHQ Compliance Guide Extracts June 2014 to present page 5 of 20

[69] RFI 34 of Documents Enclosed with Response to RFI: Secret Intelligence Service Bulk Personal Data Guidance on the Authorisation Process December 2014 to October 2015; RFI 35 Secret Intelligence Service. Bulk Personal Data. Guidance on the Authorisation Process October 2015 to present

[70] 12th Sitting of Public Bill Committee, Investigatory Powers Bill, Tuesday 26 April 2016, Column 539

53. Bulk Personal Datasets are intrusive.

54. The Respondents' Closed Response says at page 2 paragraph 4):

> '4) While each of the datasets in themselves may be innocuous intelligence value is added in the interaction between multiple datasets. **One consequence of this is that intrusion into privacy can increase.**
>
> (emphasis added)

55. The Security Service Bulk External Data Acquisition Internal Authorisation Process 2006[71] states:

> 'Senior MI5 official endorsement should be sought by the Grade 2 authoriser if they feel that the request is particularly intrusive (for example does the data include unusually large numbers of people of no intelligence interest of is the data extremely intrusive/delicate e.g. [REDACTION]).

56. The Secret Intelligence Service state in User Comms 2011 – 2014[72] document:

> '3. Bulk data exploitation can be a very powerful tool, enabling us to search across multiple data sources (e.g. [redacted]), travel, financial and telecommunications) and to identify connections between individuals. Because it may include information on untargeted individuals [redacted] **it is also potentially more intrusive than traditional targeted information**' (emphasis added).

Corporate Risk

57. In assessing risk, a high priority is placed on embarrassment to the Agencies:

- Policy for Bulk Data Acquisition, Sharing, Retention and Deletion dated October 2010[73]:

  > 'Corporate Risk refers to the potential for political embarrassment and/or damage to the reputation of MI5 and its SIA partners, data providers and HMG were it to become public knowledge MI5 holds certain datasets in bulk.
  > ...
  > Were it to become widely known that the Service held this data the media response would most likely be unfavourable and probably inaccurate.

---

[71] Document '4)' from Documents dating from June 2005 to May 2014 disclosed pursuant to paragraph 5 of the order of 15 January 2016: Security Service Bulk External Data Acquisition, Internal Authorisation Process, 2006, page 6 of 12

[72] Document '21)' from Documents dating from June 2005 to May 2014 disclosed pursuant to paragraph 5 of the order of 15 January 2016: User Comms 2011 – 2014, page 1 of 6

[73] RFI 13 of Documents Enclosed with Response to RFI: Security Service Policy for Bulk Data Acquisition Sharing Retention and Deletion, October 2010 to March 2015 page 9

- SIS Bulk Personal Data Guidance on the Authorisation Process December 2014 to October 2015[74] states:
  Factors to consider when judging level of risk:
  High when revelation would:
  - Cause HMG serious embarrassment [redacted]
  - Jeopardise foreign investment in GB
  - [redacted]
  - alienate public opinion and degrade HMG reputation;
  - have an adverse impact on SIS reputation within HMG and the public
  - damage SIS equities or reduce SIS's ability to operate effectively.

Abuses

58. The Intelligence and Security Committee report stated that abuse had taken place, reporting that 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.'*[75]

59. The Respondents Closed Response to the Claimant's Request for Further Information and Disclosure dated 15 January 2016 states on page 4 in relation to the Security Services:

> BPD Regime
> (a) In the period 1 June 2014 to 9 February 2016 six instances of non-compliance were detected:
> i. Three of these were instances of datasets mistakenly left out of the Security Service's BPD review process, with the result that the necessity and proportionality of retention was not reconsidered for between one and two years;
> ii. A further instance where a dataset which fell within the definition of 'bulk personal dataset' had not been entered into the BPD process. This dataset has now been deleted;
> iii. Two cases of individual non-compliance by staff members
>
> (b) As responsibility for BPD compliance is shared between the business, information management and technical teams, it is assessed that 12 staff members hold an element of responsibility for the non- compliance referred to at (a)(i) and (a)(ii) above. In respect of (a)(iii) the responsibility was of two individuals (one on each occasion).
>
> (c) Two of the individuals referred to at (a) have been subject to disciplinary procedures.
>
> (d) Of the non-compliance referred to at (a) above: a. Of the instances of non-compliance referred to at (a)(i), one was self-reported and the others were uncovered following further investigation by the Security Service's information management team ; b. The non-compliance referred to at (a)(ii) was identified following a review of BPD holdings; c. The two instances of non-compliance referred to at (a)(iii) were identified by the Security Service's protective monitoring team.

---

[74] RFI 34 of Documents Enclosed with Response to RFI: SIS Bulk Personal Data: Guidance on the Authorisation Process December 2014 to October 2015, page 3
[75] ISC Report, paragraph 163, citing ***

Section 94 Regime

(a) In the period 1 June 2014 to 9 February 2016 47 instances of non- compliance either with the MI5 Closed Section 94 Handling Arrangements, or internal guidance or the Communications Data Code of Practice, were detected. These involved:

i. Four errors involving issues with the necessity and proportionality case which was made for the request for Communications Data from the database pursuant to section 22 of RIPA, e.g. insufficient consideration of data relating to an individual in a sensitive profession.

ii. 43 errors involving (i) mistransposed digits in selectors; (ii) selectors that did not relate to the subject of investigation; and (iii) occasions where duplicate requests were made.

(b) As Communications Data requests commonly have a requester and an approver, it is assessed that 94 staff members hold an element of responsibility for these instances of non-compliance.

(c) No staff members have been prosecuted, dismissed or disciplined in relation to these instances of non-compliance.

(d) These instances were self-reported by the originator of the request following detection either by the originator, the authorising officer or a third party (e.g. a team member).

60. In relation to MI6 during the same period there were five instances of non-compliance and at GCHQ there were two instances of non compliance.[76]

Secret Intelligence Service

BPD Regime

(a) During the period 1 June 2014 to November 2015 five instances of non-compliance were detected:

i. Two of these were instances of datasets being ingested into the system before they were authorised. In both cases, they were removed as soon as the error was detected. [REDACTED] ii. Three cases of individual non-compliance.

(b) In respect of (a)(i) above, the two instances occurred as a result of an ambiguity with SIS's IT systems, rather than being ascribable to any staff member's failure to comply. In respect of (a)(ii) above, three staff members were identified as responsible;

(c) None of the three staff members were prosecuted or dismissed, but the three referred to at (a)(ii) above were disciplined for non- compliance;

(d) The three instances of non-compliance referred to at (a)(ii) above were identified by

[76] Respondents Closed Response to the Claimant's Request for Further Information and Disclosure dated 15 January 2016

SIS's Information Security audit team.

GCHQ

BPD Regime

(a) Two instances of non-compliance have been detected: i. The first case concerns a BPD which was acquired in 2012. The acquisition was approved, and the relevant BPDAR signed. However, the dataset was not subsequently reauthorized or considered by the BPD Review Panel, as was required. This oversight was discovered in 2015 by GCHQ's Compliance Team, who then contacted the dataset's data owners. The dataset was deleted in August 2015 as it was deemed to be no longer of use. ii. The second case was a BPD which was first acquired by GCHQ in 2010. However, it was not initially recognised as BPD. It was subsequently identified as BPD in 2015 by GCHQ's

Compliance Team in the context of using the data for training purposes. It was then brought within the BPD Regime and subjected to the relevant safeguards, forms and oversight.

(b) The instances of non-compliance were corporate, rather than individual. It is therefore not possible to ascribe responsibility to particular individuals. For the same reason there has been no disciplinary action.

(c) There have been no prosecutions, dismissals or disciplinary action.

(d) See (a) above. Section 94 Regime

(a) There have been no instances of non-compliance with the GCHQ Closed Section 94 Handling Arrangements.

(b) See (a) above.

61. GCHQ Compliance Guide Extracts[77] dated June 2014 to present states on page 10 of 19:

> What is an error?
> There is no simple definition of whether an incident constitutes an error. Many comprise interference with one of more individuals' right to privacy and result from an accident or a failure to observe GCHQ procedures.
> ...
> In a typical year GCHQ makes between 5 and 20 errors, of which only a small number may be deemed serious.

62. Insufficient information has been provided in relation to the seriousness of these breaches. Presumably, most breaches are not detected.

[77] RFI 4 of Documents Enclosed with Response to RFI: GCHQ Compliance Guide Extracts June 2014 to present

Alternative use

63. The Respondents' Response confirmed that BPDs are used for *'experimental or innovation purposes'*:

> '63) The use of BPD for *'experimental or innovation purposes'*, for example, the development of novel analytical technique or testing a new IT system, is specifically addressed at §5.4.1. The potential for increased risk to, inter alia, the security of the data and risk of additional interference with the right to privacy are acknowledged and addressed. Any such use of BPD must be specifically *'considered and authorized in advance by a senior MI5 official'*...'
>
> '190) The use of BPD for *'experimental purpose'* for example the development of a novel analytical technique or testing a new IT system, is specifically addressed at §8.1. The potential for increased risk to inter alia the security of the data and risk of additional interference with the right to privacy are acknowledged and addressed.'

64. The documents provide additional information:

GCHQ Compliance Guide Extracts 1 June 2005 to 2010 state[78]

The scope of SIGINT

> 1. ...Justification may also be framed in terms of maintaining GCHQ's technical knowledge...
>
> 8. ...At the other end of the scale, it could be justifiable to target an individual under an SD heading, if for instance, you were not interested in the individual so much as the specialist information he might (or might not) have which would enable GCHQ to refine its targeting or to expand its range of intelligence techniques.

The Retention of information Beyond the norms

> 5. Exceptional examples of retention beyond the norms may be occasioned routinely by areas of GCHQ which specializes in research and development. [REDACTED]

Sharing data

> If you wish to share operational data with a company, for example to help it develop software for GCHQ or to share raw operational data with government customers, you should read and apply the published policy and guidance and consult the relevant team accordingly.[79]

---

[78] Document '1)' from Documents dating from June 2005 to May 2014 disclosed pursuant to paragraph 5 of the order of 15 January 2016: GCHQ . Compliance Guide Extracts as at 1 June 2005 to 2010, page 19 of 59, labelled page 103

[79] Document '2)' from Documents dating from June 2005 to May 2014 disclosed pursuant to paragraph 5 of the order of 15 January 2016: GCHQ Compliance Guide extracts 2010 – June 2014 labelled page 8 of 15

Oversight

65. The Respondents Response confirms that prior to 13 March 2015 there was no statutory oversight of Bulk Personal Datasets for MI5 or MI6 or GCHQ. It states there was non-statutory oversight of the Intelligence Services Commissioner. However, it was not until 13 March 2015 that the Intelligence Services Commissioner was empowered to review the acquisition, use, retention and disclosure by the intelligence services of BPDs. It is not clear what the non statutory review consisted of.

66. Secret Intelligence Service Intranet pages since 7 November 2013 and 14 April 2014[80] states:

> 'To date there has been no external oversight of SIS's (or SIA partners') bulk data operations but options to introduce a statutory form of oversight are likely to be considered as part of legislative reform over the next 18 months. As an interim arrangement the Intelligence Services Commissioner has been asked to review (on a non statutory basis) the three agencies' arrangements for acquiring, handling and using this type of data'.

67. The Respondents' Closed Response states at page 64, paragraph 309 that it was subject to external oversight from 2011 when 'GCHQ invited the Intelligence Services Commissioner to begin ongoing scrutiny of its use of section 94 directions on a non-statutory basis.'

68. 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[81]. The Direction places the review of Bulk Personal Datasets by the intelligence Services Commissioner onto a statutory basis.

Policy

69. Policy was not agreed between the Agencies on Bulk Personal Data, according to the Respondents Closed Response, until February 2015. The Respondents Closed Response quotes extensively from this recent policy.

70. The Respondents' Closed Response states in relation to MI5 past policies and practice that:

> '86) In the period from 1 June 2014 (1 year prior to the issue of the present claim) and 4 November 2015, MI5's policies in relation to BPD were similar to those now in force.'

71. The Respondents then considers the MI5 policy in place at 1 June 2014. Whilst saying that this had been in force since October 2010 it does not state what amendments were made to the policy in the period October 2010.

---

[80] RFI 45 of Documents Enclosed with Response to RFI: Secret Intelligence Service Intranet Pages 7 November 2013 and 14 April 2014, page 2

[81] http://www.intelligencecommissioner.com/docs/PM_Direction_12_March_15.pdf

72. In respect of SIS the Respondents Closed Response states that policy and practice in place since June 2014 was **similar** to the Handling Arrangements now in force. It was only in October 2014 that a Code of Practice expressly prohibited 'self searching'.

73. In relation to GCHQ the Respondents' Closed Response refers to the Compliance Guide for the prior June 2014 onwards. Extracts prior to this period are undated.

Section 94: Bulk Communications Data

History

74. On the day the Draft Bill Investigatory Powers Bill was published, the Home Secretary announced that the Intelligence Agencies have been acquiring bulk communications data of the UK population purportedly under section 94 of the *Telecommunications Act 1984*. This has never previously been publicly admitted.

75. In the Respondents' Amended Response it was avowed that section 94 of the Telecommunications Act was used by GCHQ to collect Bulk Communications Data by means of section 94 Directions. Two such directions were made in the period 1998 to 1999 both of which were cancelled in 2001. All other such direction have been made since 2001.

76. It was avowed that the Security Service has acquired BCD by means of a number of section 94 directions. The earliest was made in 2005. Since 2005 successive Home Secretaries have issued directions under section 94 requiring certain providers of public electronic communications networks to provide MI5 with BCD.

77. The Respondents avowed in their Amended Response that since 2001 GCHQ has sought and obtained from successive Foreign Secretaries a number of section 94 directions relating to the ongoing provision of various forms of bulk communications data. It has not been clarified what is meant by 'ongoing' and whether directions have been constantly in place since 2001. The Respondents refer to use of section 94 as:

> '9) …comprehensive feed of particular types of communications data.'

78. The Respondents avowed in their Closed Response on that

> '11) Since 2005 successive Home Secretaries have issued and/or decided to maintain directions under s.94 of the 1984 Act requiring a number of CNPs to provide MI5 with [REDACTED] communications data in the interests of national security. [REDACTED]. The data obtained is aggregated in a database. Successive Home Secretaries have agreed that they would keep these arrangements under review at six-monthly intervals. The review process involves a detailed submission being made to Home Office by MI5, setting out the ongoing case for the database, including specific examples of its usefulness in the intervening period and setting out any errors in using the database which have occurred in that time."
>
> '18. Section 94 Directions were first laid in respect of the database on 21 July 2005. The view of successive Home Secretaries has been that disclosure of the Section 94 Directions in respect of the database would be against the interests of national security. Although the fact that Section 94 Directions have been issued has been avowed, the

direction themselves have not been published [REDACTED]. The directions **remain in place** but are reviewed every six months.'

79. The Respondents state in their Closed Response that:

> 2) A number of directions have been issued under section 94 of the 1984 Act. **Such directions** which fall within the scope of the present Claim are addressed below. These are essentially directions which involve the acquisition/use of Bulk Communications Data ("BCD").

80. It is not clear whether there are directions that have been made under section 94 which the Respondents' believe do not 'fall within the scope of the present Claim'.

81. In relation to whether the use of section 94 has been disclosed in previous proceedings, the Respondents' 'Closed Response to the Claimants' Request for Further Information and Disclosure Dated 15 January 2016' states that:

> 'GCHQ's Compliance Guide was exhibited in full to the CLOSED GCHQ witness statement...That contained passages which referred to the use of section 94 directions to obtain bulk communications data e.g. in the 'Authorisations', 'Collection and data acquisition' and 'Communications Data' sections of Compliance Guide'.

Traffic data and Service Use Information

82. The Respondents state at paragraph 225 of the Closed Response, page 46, that communications data provided by the CNPs under the section 94 directions is limited to "traffic data" and "Service Use Information".

> The information to which the MI5 Closed Section 94 Handling Arrangements relate is defined in section 2. §2.1 notes that the communications data provided by the CNPs under the Section 94 Directions is limited to "traffic data" and "Service Use Information" (as defined in §3.11, citing section 21(4)(a) and (b) of RIPA) [REDACTED].

83. The definition of communications data appears to vary slightly in the disclosure but refers to non content data in general. It is not clear whether understanding of what constitutes Bulk Communications Data has changed over time. The more recent documents refer to the RIPA definitions. It is not clear why the Respondents do not state in the Response that communications data includes "Subscriber Information" as per RIPA.

84. The Security Service Bulk Personal Data Guidance November 2015[82] refers to:

> 'The extent of meta data v content data'
> Footnote: meta data – meaning the combination of Communications Data and Content Meta Data.

[82] RFI 16 of Documents Enclosed with Response to RFI: Security Service Bulk Personal Data Guidance, page 15 of 20

85. The disclosure states in relation to traffic data in GCHQ Compliance Guide Extracts as at 1 June 2005 to 2010[83]:

> 'Footnote: Traffic data in relation to any communication, means (a) any data identifying or purporting to identify, any person, apparatus or location to or from which the communication is or may be transmitted, (b) any data identifying or selecting or purporting to identify or select apparatus through which or by means of which the communication is transmitted (c) any data comprising signals for the actuation of apparatus used for the purposes of telecommunication system for affecting (in whole or in part) the transmission for any communication and (d) any data identifying the or other data as data comprised in or attached to a particular communication.'
>
> '(c) any other information that is held or obtained in relation to persons to who he provides the service, by a person providing a telecommunications.
> Footnote: Historical data such as credit card details of bill payee or the email address owner would fall within this category'.

86. The GCHQ compliance guide extracts 'Relevant extracts from the 'Communications data' section of the compliance guide as at June 2014[84] states:

> Communications data comprises traffic data, service use data and subscriber data.
> Traffic data is data attached to a communication for the purposes of any telecommunications system used to transmit it.
> Service use data is any non-content information about the use made of a telecommunication service by a person and
> Subscriber data is any other information held by a provider about a person to whom it provides a telecommunication service.

87. The Respondents' Closed Response states that:

> 13) The data provided does not contain communication content or Subscriber Information (information held or obtained by a CNP about persons to whom the CNP provides or has provided communications services). The data provided is therefore anonymous. It is also data which in any event maintained and retained by CNPs for their own commercial purposes (particularly billing and fraud prevention).

Intrusiveness of BCD

88. The ISC report dated March 2015 remarked:

> *"We were surprised to discover that the primary value to GCHQ of bulk interception was not in reading the actual content of communication, but in the information associated with those communications."*[85]

---

[83] Document '1)' from Documents dating from June 2005 to May 2014 disclosed pursuant to paragraph 5 of the order of 15 January 2016: GCHQ Compliance Guide Extracts as at 1 June 2005 to 2010, labelled page 207, page 47 of 59

[84] RFI 4 of Documents Enclosed with Response to RFI: GCHQ Compliance Guide Extracts June 2014 to Present, page 9 of 20

[85] ISC Report paragraph 80

89. Smartphone, laptops and electronic devices have changed how we communicate and interact with others, express ourselves and record and remember our thoughts and experiences. These devices have become prime targets for GCHQ, MI5 and MI6.

90. The communications data will potentially include the who, what, where, when and how relating to every communication that a person has online. This includes but is not limited to visited websites, email contacts, to whom, where and when an email is sent, map searches, GPS location, and information about every device connected to every wifi network in the United Kingdom, which includes Smart Tech such as Nest, iKettle, Smart Barbit, Amazon Echo and others.

91. Bulk Communications data can provide vast knowledge about individuals, particularly when cross-checked against other public records.

92. Retention of details of every website visited reveals much more about a person. It can be used to profile them and identify preferences, political views, sexual orientation, spending habits and much more. This is plainly sensitive personal information and it is clearly a huge invasion of privacy to collect and retain this information on innocent people.

93. The Respondents' Disclosure states that they do store web browsing history in a similar way proposed in the Investigatory Powers Bill:

> "Communications data includes Internet addresses to the extent that they identify a network or host computer. It does not include page content hosted on that site."[86]

Policy

94. In relation to past policies of MI5 the Respondents Closed Response states that ' 264) Neither MI5's process or policy in relation to Section 94 of the 1984 of the Act have changed materially in the relevant period'. The relevant period appears to refer to June 2014 onwards and not prior to this.

95. The Respondents state that:

> 16) Data is provided by CNPs on a regular basis. Data is retained by MI5 for 12 months before being deleted.

Safeguards

96. Not only has the use of the power been far from transparent, there has and is, given that this power is still in operation, no meaningful or effective oversight regime: no statutory review by the Commissioner; no provision for a review of directions; no Code of Practice; no judicial authorisation; and the directions do not expire. David Anderson QC in *A Question of Trust* said:

> 6.17 ... s94... is very broad in nature and imposes no limit on the kinds of direction that

[86] Document '1)' from Documents dating from June 2005 to May 2014 disclosed pursuant to paragraph 5 of the order of 15 January 2016: GCHQ Compliance Guide Extracts as at 1 June 2005 to 2010, labelled page 207, Footnote 2

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.

97. The Interception of Communications Commissioner, asked in 2015 by Prime Minister David Cameron to oversee section 94 directions, pointed to the lack of a central record, which raises concern about the ability to carry out effective oversight in any event[87]:

"there does not appear to be a comprehensive central record of the directions that have been issued by the various Secretaries of State".

Sharing

98. Existing practice is that entire Bulk Personal Datasets, including those relating to British Citizens may be shared with foreign intelligence agencies. Most safeguards are lost on sharing. As the ISC explains:

'...while these controls apply within the Agencies, they do not apply to overseas partners with whom the Agencies may share the datasets.' [88]

99. Given the relationship our intelligence agencies enjoy within the Five Eyes, it is assumed a number of Bulk Personal Datasets will have been shared.

Proposals in the Investigatory Powers Bill

100. It is proposed that obtaining and use of personal datasets will be authorized by warrant in bulk by reference to a "class" of such datasets (c.177). These can be added to by specific personal data set warrants (c.178).

101. Part 7, Clause 175 of the Bill provides that bulk personal datasets are authorized by class based warrants – these warrants do not name individuals or addresses but rely on generalized categories of people or places.

102. Part 7 of the IPB, BPD is defined at section 174. There are two types of BPD warrant outlined at section 175(4). Subsection (a) provides for 'a class BPD warrant' which allows the Intelligence Services to obtain, retain or examine bulk personal datasets that fall within in class described in the warrant, whilst section 175(4)(b) provides for 'a specific BPD warrant' which authorizes the production of a specific BPD described in the warrant.

---

[87] http://www.iocco-uk.info/docs/2015%20Half-yearly%20report%20(web%20version).pdf
[88] ISC Report page 58 paragraph 163

103. Under s.177 class-based warrants are to be issued only where examination of that 'class ' of data is deemed proportionate and necessary for operational purposes related to the three broad headings of national security, serious crime or the economic well-being of the UK related to national security.

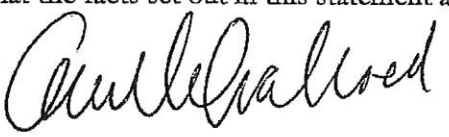
104. Bulk Personal Datasets would be obtained through a specific BPD Warrant [Clause 178] and class BPD warrant [Clause 177]. A class warrant authorizes an intelligence service to obtain, retain or examine bulk personal datasets that fall within a class described in the warrant. A class warrant must include a description of the Bulk Personal Datasets to which it relates and an explanation of the operational purpose for which the applicant wishes to examine the data collected.

105. Collection of BCD is also part of the Investigatory Powers Bill, being addressed in Part 6, Chapter 2.

106. The use of Section 94 is reflected in Part 9 Chapter 1 of the Investigatory Powers Bill [Clause 216, 21 – 220], National Security Notices and Maintenance of Technical Capability.

STATEMENT OF TRUTH

I believe that the facts set out in this statement are true.

SIGNED: 

DATED: 3. May 2016