REPORT OF THE BULK POWERS REVIEW

by

DAVID ANDERSON Q.C.

Independent Reviewer of Terrorism Legislation

Presented to Parliament
by the Prime Minister
by Command of Her Majesty

August 2016

Cm 9326

This publication is available at www.gov.uk/government/publications

Print ISBN 9781474136914
Web ISBN 9781474136921

ID 12081633 08/16 56730 19585

Printed on paper containing 75% recycled fibre content minimum

Printed in the UK by the Williams Lea Group on behalf of the Controller of Her Majesty's Stationery Office

CONTENTS

ANNEXES

EXECUTIVE SUMMARY

- **This Report evaluates the operational case for four of the powers in the Investigatory Powers Bill currently before Parliament: bulk interception, bulk acquisition, bulk equipment interference and bulk personal datasets. These powers can be used only by MI5, MI6 and GCHQ.**
- **It provides a full introduction to each of the powers (chapter 2) and notes the generally favourable conclusions of those security-cleared persons who have in the past commented on their utility (chapter 3).**
- **The security-cleared Review team comprised technical, investigatory and legal experts. We consulted widely. Each member of the Review team authorises me to say that they are in agreement with the conclusions of this Report and with my recommendation (1.28-1.55).**
- **The Review applied itself in particular (chapter 4) to:**
    - **some 60 detailed case studies provided by MI5, MI6 and GCHQ, together with associated intelligence reports,**
    - **internal documents from each of the Agencies, in which the utility of the powers was discussed, and**
    - **the questioning of some 85 intelligence officials, including on whether other methods could have achieved the same results.**
- **The Report concludes that there is a proven operational case for three of the bulk powers, and that there is a distinct (though not yet proven) operational case for bulk equipment interference (9.12-9.15).**
- **As the case studies show, the bulk powers are used across the range of Agency activity, from cyber-defence, counter-espionage and counter-terrorism to child sexual abuse and organised crime (Annexes 8-11).**
- **The bulk powers play an important part in identifying, understanding and averting threats in Great Britain, Northern Ireland and further afield. Where alternative methods exist, they are often less effective, more dangerous, more resource-intensive, more intrusive or slower (chapters 5-8).**
- **The Review was not asked to reach conclusions as to the proportionality or desirability of the bulk powers. As the terms of reference for the Review made clear, these are matters for Parliament (1.10-1.14).**
- **The Report makes a single recommendation: that a Technical Advisory Panel of independent academics and industry experts be appointed by the Investigatory Powers Commission to advise on the impact of changing technology, and on how MI5, MI6 and GCHQ could reduce the privacy footprint of their activities (9.16-9.31).**
- **Though it found that the bulk powers have a clear operational purpose, the Report accepts that technological changes will provoke new questions. Adoption of its Recommendation will enable such questions to be asked, and answered, on a properly informed basis (9.32).**

1. INTRODUCTION

Subject-matter of the Review

1.1. This is the report of the Independent Bulk Powers Review **[the Review]**. The Review was set up in May 2016 to evaluate the operational case for the four bulk powers **[the powers under review]** for which provision is made in Parts 6 and 7 of the Investigatory Powers Bill currently before Parliament **[the Bill]**.[1] Those powers relate to bulk interception, bulk acquisition, bulk equipment interference **[bulk EI]** and bulk personal datasets **[BPDs]**.[2]

1.2. The powers under review are distinguished from other powers in the Bill by their "*bulk*" nature (1.4-1.9 below), and by the fact that the data for whose collection and/or retention they provide may be accessed only by the Security and Intelligence Agencies **[SIAs]**: that is, the Security Service **[MI5]**, the Secret Intelligence Service **[MI6]** and the Government Communications Headquarters **[GCHQ]**.[3]

1.3. According to a recent report, the UK is one of five EU Member States that have detailed laws authorising the carrying out "*not only targeted surveillance but also signals intelligence"* – in other words, to conduct activities similar to at least some of the powers under review.[4] Such activities are also conducted elsewhere in the world, e.g. by the USA, Russia, China and Israel.

What are bulk powers?

1.4. The phrases "*bulk"* and "*bulk power*" trip readily off the tongue but are not defined in the Bill, and merit analysis.

1.5. For NGOs and others, the defining feature of a bulk power is that it allows public authorities (in particular, law enforcement and intelligence) to have access for specified purposes to large quantities of data, *a significant portion of which is not*

---

1 All references to the Bill in this Report are to the version of 8 June 2016 introduced to the House of Lords.

2 A full list of the acronyms used in this report is at Annex 1.

3 MI5 investigates and disrupts people, mostly within the UK, who pose threats to national security (including terrorism, espionage, cyber threats and proliferation). MI6 collects intelligence and conducts covert activity globally in support of the UK's foreign, defence and security policies. GCHQ gathers intelligence from communications globally, reporting across a wide range of requirements including counter-terrorism, counter-proliferation, foreign intelligence and serious crime. It also protects Government communications and communications networks. Each SIA has an informative and accessible website.

4 The other four are Germany, France, the Netherlands and Sweden: EU Agency for Fundamental Rights, *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU* (2015), pp. 20-24. The authors cautioned that the list may not be exhaustive: it is possible that other states conduct such activities without the benefit of detailed legislation.

associated with current targets.[5] An example falling outside the scope of the Bill is the police power to access CCTV footage of a busy street over a given period, whether filmed by a public authority or a business, for the purposes of investigating or prosecuting a reported crime.

1.6. In the context of the powers contained in the Bill – "*the interception of communications, equipment interference and the acquisition and retention of communications data, bulk personal datasets and other information*"[6] – the exercise of a bulk power implies the collection and retention of large quantities of data which can subsequently be accessed by the authorities. On this broad definition, the characterisation of a power as a bulk power does not depend on whether data is collected and stored by the Government or by a private company.[7] Applying that definition, the Bill could be said to contain bulk powers other than the four I have been asked to look at: see 2.5 below.

1.7. But the Bill (and this Review's terms of reference) proceed on a narrower definition of bulk powers, limited to those powers which provide for data in bulk to be acquired by the Government itself. On that narrower basis, powers to require (for example) providers of telephone and internet services to collect and retain their customers' data in bulk do not qualify as bulk powers, even when intelligence or law enforcement have the power to acquire that data.[8]

1.8. The narrower definition is mirrored in US practice. Thus, the National Academy of Sciences in its Report of 2015 distinguishes the bulk collection of signals intelligence by the US government from the government's use of "*bulk data held by other parties*", which it looks upon as a possible substitute for bulk collection rather than a form of bulk collection in itself.[9] Others take a similar approach.[10]

---

5 The italicised phrase is taken from the working definition of bulk collection used by the US National Academy of Sciences in its influential report, "Bulk collection of signals intelligence: technical options" (Washington DC, 2015) **[the NAS Report]**. Liberty adopted a similar broad definition of bulk in its submission to the Review of 31 July 2016, paras 10-11. The NAS Report commented (at p. 2) that "*There is no precise definition of bulk collection, but rather a continuum, with no bright line separating bulk from targeted.*": for an illustration, see 2.19(a) below.

6 Long title to the Bill.

7 The point is illustrated by the filtering arrangements provided for in clauses 63-65 of the Bill, which will permit public authorities to make complex queries of databases held by multiple service providers, thus emulating at least to some extent the ability of SIAs to interrogate a single, aggregated database enabled through the bulk acquisition power.

8 See also the Government's "Operational Case for Bulk Powers" (March 2016: see 1.14 below), which at 2.1 answers the question "*What are bulk powers?*" by exclusive reference to techniques used by the Agencies to *acquire* information in large volumes.

9 NAS Report, section 4.3, p. 57.

10 Thus, the USA FREEDOM Act ended the central holding of bulk telephone records under FISA s215, but established a new system for government access to call detail records held by service providers: Privacy and Civil Liberties Oversight Board **[PCLOB]**, Recommendations Assessment Report, 5 February 2016, p.3. Only the former programme is considered by the PCLOB to involve bulk collection.

Suggestions that the USA has been "*moving away from bulk*" must be seen in the light of this narrow meaning of the term: see further 3.63-3.65 below.

1.9. Whether a broader or narrower definition is preferred, it should be plain that the collection and retention of data in bulk does not equate to so-called "*mass surveillance*". Any legal system worth the name will incorporate limitations and safeguards designed precisely to ensure that access to stores of sensitive data (whether held by the Government or by communications service providers **[CSPs]**) is not given on an indiscriminate or unjustified basis.[11] Such limitations and safeguards certainly exist in the Bill.

Terms of reference

1.10. The terms of reference for the Review were decided upon by the Home Secretary, in consultation with the Opposition, and set out in the document at Annex 2. This states:

> "The review will examine the operational case for the investigatory powers contained in Parts 6 and 7 of the Investigatory Powers Bill, including the 'Operational Case for Bulk Powers' document which was published alongside the Bill at Introduction on 1 March. The review will report to the Prime Minister, with a copy sent to the Intelligence and Security Committee of Parliament (ISC). It will build on the previous reviews by the ISC, David Anderson QC and the Surveillance Panel convened by the Royal United Services Institute. The review will inform Parliament's consideration of the need for the bulk powers in the Bill.
>
> The review shall consider the operational case for:
>
> i. Bulk Interception
> ii. Bulk Equipment Interference
> iii. Bulk Acquisition (Communications Data)
> iv. Bulk Personal Datasets."

The requirements of the Terms of Reference as regards process are reproduced in 1.28 below.

1.11. As will be apparent, the function of this Review is limited to consideration and discussion of the operational case for the powers under review. I am not asked to opine on:

(a) what safeguards it is appropriate to place upon the powers under review; or

[11] The Shadow Home Secretary, Rt Hon Andy Burnham MP, said in the second reading debate "*it is lazy to label the Bill as a snoopers' charter or a plan for mass surveillance.*": Hansard HC 15 March 2016, vol 607 col 825. Joanna Cherry QC MP for the SNP preferred the term "*suspicionless surveillance*": col 840.

(b) whether the safeguards contained in the Bill are sufficient to render them proportionate for the purposes of the European Convention on Human Rights **[ECHR]** or European Union **[EU]** law.

These limitations were confirmed by the Security Minister's answer of 6 July 2016 to a parliamentary written question.[12]

1.12. On the other hand, my brief is wide enough to allow me to consider not only whether there is an operational case for the powers, but, in relation to each power, the strength or otherwise of any such operational case.

1.13. In assessing the operational case as mandated by my terms of reference, I have also sought to have regard to what alternative means might have been used to achieve the operational results that are claimed for the powers under review. This consideration of the necessity of the powers under review accords with the exchange of letters between Government and Opposition that preceded the establishment of the Review (Annex 3), and with the debate at Report stage in the House of Commons.[13]

1.14. The terms of reference refer to a document entitled "Operational Case for Bulk Powers" **[the Operational Case]**. The Operational Case was published as a 47-page open document alongside the Bill on 1 March 2016, and additional classified material was made available to the ISC.[14] Along with each member of the Review team, I have studied and interrogated both the Operational Case and the additional material provided to the ISC. As will be seen, the SIAs did not limit themselves to the examples in that document when selecting case studies for us to examine.[15]

---

12 Asked by Roger Godsiff MP whether the Home Secretary would "*establish a further review of, or extend the remit of the current review to include, the proportionality of the powers currently included in the Investigatory Powers Bill*", the Security Minister replied: "*The current review being conducted by David Anderson QC is specifically examining the operational case for the bulk powers in Parts 6 and 7 of the Investigatory Powers Bill. The review will not include a consideration of the safeguards that apply to these powers, and associated questions of proportionality, as that is rightly a matter for Parliament to consider as part of its scrutiny of the Bill.*"

13 In the words of Keir Starmer QC MP, speaking for Labour, "*the review team's ability to assess whether the same result could have been achieved through alternative investigative methods is important to that exercise and the confidence that we can have in the outcome*": Hansard HC 7 July 2016, vol 611 col 1069. This appears to be what the Security Minister, John Hayes MP, had in mind when he said immediately beforehand: "*That is why the focus on necessity and not merely utility is so important.*"

14 The Operational Case is available, along with other "*over-arching documents*" relating to the Bill and published on 1 March, from https://www.gov.uk/government/publications/investigatory-powers-bill-overarching-documents. Operational cases for the retention of internet records and for the use of communications data by public authorities were also published by the Government, in November 2015 and July 2016 respectively.

15 Contrast the Operational Case with Annexes 8-11.

The Investigatory Powers Bill

1.15. This Review was conducted during the passage of the Bill**,** which was introduced to Parliament after extensive pre-legislative scrutiny on 1 March 2016.

1.16. The need for a comprehensive Bill to govern investigatory powers had been identified in three studies published between March and July 2015. One of those studies was my own "A Question of Trust" **[AQOT]**, which I produced over a period of nine months with the help of a different small team.[16] The Bill, which on arrival in the House of Lords extended to nine Parts, 243 clauses, 10 schedules and 253 pages,[17] seeks to give effect to my central recommendation that:

> "A comprehensive and comprehensible new law should be drafted from scratch, replacing the multitude of current powers and providing for clear limits and safeguards on any intrusive powers that it may be necessary for the public authorities to use."[18]

1.17. The impetus for those recommendations derived in part from the well-known activities of Edward Snowden. I neither condone Edward Snowden's actions nor underestimate the damage that they have done, on which I have been briefed. Nonetheless, the material taken by him through access to US National Security Agency **[NSA]** systems, and the articles subsequently published in outlets including the Guardian and the New York Times, have been the basis for suggestions that in the UK as elsewhere, broad and obscure powers were being exercised in a manner that few had understood. Litigation, fuelled by those allegations, has persuaded the IPT to indicate that some powers have lacked the necessary accessibility and foreseeability to comply with international human rights standards. That in turn has driven the Government to accept, in the Bill and its accompanying documents, that much greater transparency is needed. One of the purposes of AQOT, and in particular my proposal for a powerful new regulator, was to ensure that Parliament and the public are properly and sufficiently informed, as democracy requires, about the powers being exercised in their name.

---

16 AQOT is available from my website: https://terrorismlegislationreviewer.independent.gov.uk/. The other two studies were a report of March 2015 by the Intelligence and Security Committee of Parliament **[ISC]** entitled "Privacy and Security" **[2015 ISC report]**, which in accordance with the remit of the ISC dealt only with the powers of the SIAs, and a Royal United Services Institute report of July 2015 "A Democratic Licence to Operate" **[RUSI report]**. The RUSI panel was a wide-ranging one and included former heads of each SIA: but unlike the ISC and my own review, it had only limited access to classified material.

17 This is the version of the Bill to which I refer throughout this report: see fn 1 above.

18 AQOT, Executive Summary, para 10; cf. Home Secretary's Foreword to Draft Investigatory Powers Bill, 4 November 2015.

1.18. The powers proposed in the Bill comprise, in rough outline:

(a) powers to intercept communications to replace those currently provided for (sometimes opaquely) by Part I Chapter 1 of the Regulation of Investigatory Powers Act 2000 **[RIPA 2000]** and the Wireless Telegraphy Act 2006 **[WTA 2006]**;[19]

(b) powers to require the retention of and access to communications data, to replace those currently provided for pursuant to:

- the Telecommunications Act 1984 **[TA 1984]** (bulk acquisition of communications data);
- Part I Chapter 2 of RIPA 2000 (targeted communications data acquisition);
- the Data Retention and Investigatory Powers Act 2014 **[DRIPA 2014]** and the Anti-Terrorism Crime and Security Act 2001 (communications data retention); and
- some 65 other statutory mechanisms;[20]

(c) a completely new power to require the retention of internet connection records **[ICRs]**;[21]

(d) powers of equipment interference **[EI]** (otherwise known as Computer Network Exploitation **[CNE]**) based on those possessed by the police under the Police Act 1997 and the SIAs under the Intelligence Services Act 1994 **[ISA 1994]**;[22] and

(e) the power of the SIAs to retain and use BPDs obtained pursuant to the Security Service Act 1989 **[SSA 1989]** and ISA 1994.[23]

1.19. Though exercised in some cases under laws which I have described as "*incomprehensible save to a tiny band of initiates*",[24] it is fair to say that the great majority of these powers are already in use. An important exception is the power to require the retention of ICRs (1.18(c) above). A further exception is

---

19 Part 2 and Part 6 Chapter 1 of the Bill.

20 Part 3, Part 4 and Part 6 Chapter 2 of the Bill. The 65 statutory mechanisms are identified at AQOT 6.18 and Annex 6.

21 Clauses 59(6) and 83(9). ICRs are a type of communications data, but are here listed separately because the power to require their retention is new.

22 Part 5 and Part 6 Chapter 3 of the Bill.

23 Part 7 of the Bill.

24 AQOT Executive Summary, para 35. The former Attorney General Dominic Grieve QC MP went further, remarking that "*even the initiates sometimes found it incomprehensible*": Hansard HC 25 June 2015, vol 597 col 1092.

equipment interference in bulk, one of the powers under review. I am told that to date, GCHQ has carried out only EI operations for which it has been possible to provide sufficient description of the operational plan and associated safeguards to ensure that the Secretary of State could understand the precise level of intrusiveness in detail, and thus be able to conclude that all of the proposed activity was necessary and proportionate. Such operations would have been authorised under a targeted EI warrant under the IP Bill.[25]

1.20. The Bill stands not only for transparency but for the introduction of significant new safeguards. These include, among many others:

(a) the principle that warrants should enter into force only after approval by a judge; and

(b) the creation of a powerful new regulatory and supervisory body, headed by the Investigatory Powers Commissioner, which I will refer to as the Investigatory Powers Commission **[IPC]**;[26] and

(c) additional protections for the communications of certain sensitive professions and groups such as lawyers, journalists and MPs.

The principal safeguards applicable to the powers under review are summarised at 2.25-2.26, 2.43, 2.66-2.67 and 2.82-2.86 below. It remains to be seen whether further safeguards will be needed in relation to certain capabilities (e.g. for accessing communications data) as a consequence of EU law.[27]

1.21. The Bill does not cover other forms of surveillance activity (e.g. use of directed surveillance, intrusive surveillance, property interference, covert human

---

25 This is consistent with the reference in the 2016 ISC Report to bulk EI being required for "*future-proofing*" (paras 15-16), and to the hypothetical nature of the case studies both in the Operational Case and as presented to us.

26 An SNP amendment that would have formally created an Investigatory Powers Commission was rejected in the House of Commons by 281-64 (Hansard HC 6 June 2016, vol 611 cols 899-902, 929-931). But the Government itself anticipated when launching the draft Bill that the new oversight body "*will be called the Investigatory Powers Commission*" (*Factsheet – Investigatory Powers Commission*, November 2015), and it may be a useful precedent that the Interception of Communications Commissioner's office has become known as IOCCO, to reflect the fact that many of its functions are discharged not personally by the Commissioner but by its permanent staff, including its skilled inspectorate.

27 See Case C-698/15 *Secretary of State for the Home Department v Tom Watson and others* ECLI:EU:C:2016:572, Opinion of the Advocate General, 19 July 2016, paras 216-245. That Opinion concerned the DRIPA 2014 powers, now in Parts 3 and 4 of the Bill: the principal safeguards pressed by the Advocate General, including prior independent approval and a ban on use for the investigation of ordinary (non-serious) crime, already exist in relation to the powers under review. See further 2.28 below.

intelligence sources **[CHIS]**, surveillance cameras),[28] or the use of SIA powers under SSA 1989 or ISA 1994 for purposes other than intelligence collection.

1.22. The draft Bill published on 4 November 2015 received pre-legislative scrutiny from the ISC, the House of Commons Science and Technology Committee and a Joint Bill Committee of both Houses. Each of those committees reported in February 2016,[29] and their recommendations were reflected in the Bill introduced on 1 March. Between second reading on 15 March and report stage on 6-7 June, a House of Commons Public Bill Committee considered the Bill over 16 half-day sittings.[30] The Joint Committee on Human Rights produced its own report on 2 June.[31] Further reports on specific aspects were issued in July 2016 by the House of Lords Constitution Committee[32] and the House of Lords Delegated Powers and Regulatory Reform Committee.[33] The first five of these seven committees took written and oral evidence, which save in the case of the ISC (whose inquiry was into classified issues and which accordingly took evidence only in closed session) was published on their websites. The written evidence and transcripts of oral evidence before the Joint Bill Committee alone occupy 2,364 pages.[34]

Genesis of the Review

1.23. On 26 May 2016, the Shadow Home Secretary (Rt Hon Andy Burnham MP) published a letter he had written to the Home Secretary welcoming her agreement to establish this review. As his letter implied I had already been asked and agreed to lead the review, for which preparatory work was well advanced.

1.24. Terms of reference (Annex 2) were subsequently agreed by the Prime Minister, and the Review was announced by the Home Secretary when the Bill reached report stage in the House of Commons, on 7 June 2016. An exchange of letters dated 6 June 2016 between Sir Keir Starmer QC MP, Shadow Home Office Minister, and Rt. Hon. John Hayes MP, Minister of State for Security (Annex 3), was placed in the House of Commons Library. I undertook to complete the

---

28 On these techniques and the legal regime that will continue to govern them, see AQOT 8.4-8.37.

29 House of Commons Science and Technology Committee report, "Investigatory Powers Bill: Technology Issues", Third Report of Session 2015-16 (HC 573, 1 February 2016); ISC, "Report on the draft Investigatory Powers Bill (9 February 2016) **[2016 ISC report]**; Joint Committee on the Draft Investigatory Powers Bill, "Draft Investigatory Powers Bill" (HL Paper 93, HC 651, 11 February 2016).

30 Its deliberations are summarised in House of Commons Library Briefing Paper no. 7578 (Joanna Dawson), 2 June 2016, "Investigatory Powers Bill: Committee Stage Report".

31 Joint Committee on Human Rights, "Legislative Scrutiny: Investigatory Powers Bill" (HL Paper 6, HC 104, 2 June 2016).

32 Constitution Committee, *Investigatory Powers Bill*, 3rd report of 2016-17, July 2016, HL 24.

33 2nd report of 2016-17, July 2016, HL Paper 21, paras 10-28.

34 http://www.parliament.uk/draft-investigatory-powers.

Review in time for it to be considered when Parts 6 and 7 of the Bill reached committee stage in the House of Lords, now scheduled for early September.

Relevance of "A Question of Trust"

1.25. AQOT touched on the subject-matter of the Review but, for various reasons, did not seek to evaluate the operational case or the necessity for the full range of powers that it is now sought to provide for in law. In summary:

(a) I expressed firm positive views, supported by annexed material, on the utility of the ***powers to obtain and retain communications data*** that appear in Parts 3 and 4 of the Bill (AQOT 14.14-14.22 and Annexes 10-14). But those powers form no part of the Review, and in any event my views on them appear to be largely uncontroversial.[35]

(b) In relation to ***ICRs***, I noted that I had not been provided with a "*sufficiently compelling operational case*", giving full consideration to alternative means of achieving the stated purposes. I recommended that no detailed proposal should be put forward until that exercise had been performed, adding that there should be no question of progressing proposals for the compulsory ***retention of third party data*** before such time as a compelling operational case may have been made, which it had not (AQOT 14.33; Recommendations 15 and 18).[36]

(c) I expressed the clear view, on the basis of my own scrutiny at GCHQ of contemporaneous intelligence reports and questioning of desk officers and analysts who had been concerned with a number of real-life cases presented to me by the SIAs, that the ***bulk interception*** power now provided for in Part 6 Chapter 1 of the Bill had been of utility in fighting terrorism (AQOT 14.45 and Annex 9). But I noted the primacy in this area of the ISC, the Interception of Communications Commissioner **[IOCC]** and the Investigatory Powers Tribunal **[IPT]**, each of which had recently analysed and commented on regimes for bulk data collection (AQOT 14.39-14.41). Nor did I address myself to the necessity or proportionality of that power, or analyse whether the same objectives could have been achieved by less intrusive alternative methods.

---

35 Indeed the CJEU in *Digital Rights Ireland*, a judgment critical in other respects of the EU regime for the retention of communications data in bulk, referred to data retained under the Directive as "*a valuable tool for criminal investigations*" which afforded the authorities "*additional opportunities to shed light on serious crime*": Joined Cases C-293/12 and C-594/12, EU:C:2010:512, Judgment at para 49; see the discussion in AQOT 5.63-5.69.

36 In accordance with this recommendation, a 26-page operational case for the retention of ICRs was published alongside the draft Bill in November 2015.

(d) The ***bulk acquisition*** capability which MI5 and GCHQ had under s. 94 TA 1984 was not publicly avowed until November 2015: so though I had been fully briefed on it, it was (in accordance with AQOT 1.24) not mentioned in AQOT. I said on the day of the avowal that the SIAs considered the power to be useful but that their claims were yet to be scrutinised by the IOCC and the IPT. I added that "*it is absolutely right that they should have to defend that power in the public space where people evaluate the claims they make and evaluate the risks as well as the benefits*."[37]

(e) The remit of AQOT was limited to communications data and interception (AQOT 1.11), so two of the four powers under review – ***bulk EI*** (Part 6 Chapter 3 of the Bill) and ***BPDs*** (Part 7 of the Bill) – fell outside its scope and were only referred to in passing.[38]

1.26. The extent to which I had and had not expressed views on the operational case for the powers in the Bill was set out in my written evidence to the Joint Bill Committee of January 2016, in which I endorsed evidence already given to that Committee on behalf of Open Rights Group and Privacy International to the effect that the Government:

> "should do more to make an operational case for the bulk powers that it seeks to preserve … not only in the secret environment of ISC and [Investigatory Powers Tribunal] closed hearings but, to the maximum extent possible, to Parliament and the public".[39]

As I pointed out, such an approach would be in keeping with my previous advice that public authorities (including the SIAs) should "*consider how they can better inform Parliament and the public about why they need their powers, how they interpret those powers, the broad ways in which those powers are used and why any additional capabilities may be required*", and that they should contribute to any consultations on the new law "*so as to ensure that policy-making is informed by the best evidence*".[40]

1.27. In summary, I have previously expressed an evidence-based view on the utility of bulk interception, one of the four powers under review, but did so without the expert assistance that has been made available to this Review. As I said at the outset of the Review, I have approached my task on the basis that I am "*not too*

---

37 https://terrorismlegislationreviewer.independent.gov.uk/the-big-reveal/#more-2496.

38 Though I noted (again uncontroversially) that when material within databases is aggregated, it becomes a powerful tool in the hands of investigators: AQOT 8.28.

39 Supplementary evidence of David Anderson Q.C. to the Joint Draft Bill Committee, IPB 0152, 7 January 2016, paras 4-11: http://www.parliament.uk/documents/joint-committees/draft-investigatory-powers-bill/written-evidence-draft-investigatory-powers-committee.pdf.

40 AQOT, Recommendation 122.

proud to change my mind" about the bulk interception power.[41] I have not previously expressed a view on the operational case for the other three powers under review. My approach to the Review has been based on an open (if not entirely empty) mind, and a determination to follow the evidence wherever it may lead.

Working methods

Terms of reference

1.28. The terms of reference at Annex 2, which were discussed with me so far as they relate to process, state as follows:

> "The review will be undertaken by David Anderson QC, supported by a security-cleared barrister, technical expert and a person with experience of covert investigations.
>
> The Government and the Security and Intelligence Agencies will provide all necessary information, access and assistance as is needed for David Anderson QC to undertake his review effectively.
>
> David Anderson QC will report to the Prime Minister on the findings of his review in time for those findings to inform Lords Committee consideration of Parts 6 and 7 of the Bill. A copy of the report should also be provided to the ISC at this time. The Prime Minister will make the final decision as to whether the report, or parts of it, can be published without prejudicing the ability of the Security and Intelligence Agencies to discharge their statutory functions. There may be a classified annex that should also be submitted to the Prime Minister and copied to the ISC."

1.29. Within those constraints, on which I was consulted and had some influence as they were finalised, I was given a free hand to choose my team and my working methods. Each had to be appropriate to the tight schedule and the need for security clearance.

The Review team

1.30. To be of real value, it was clear that this review would require access to very highly classified material. To obtain DV (developed vetting) security clearance takes in the region of six months, or four months if expedited. It was therefore necessary to recruit team members who already had the requisite clearance to DV level or above.

[41] In a tweet, picked up by the Liberty blog on 22 June 2016: https://www.liberty-human-rights.org.uk/news/blog/investigatory-powers-bill-government-has-set-review-bulk-powers-impossible-task.

1.31. I was also conscious that the team required a variety of skills and competences, in particular:

(a) a person with the necessary technical background to understand the SIAs' systems and techniques, and the uses to which they could be put;

(b) an investigator with experience as a user of secret intelligence, including intelligence generated by the SIAs; and

(c) independent counsel with the skills and experience to challenge forensically the evidence we were shown and the case studies with which we were presented by the SIAs.

1.32. Fortunately, and despite the compressed timescale, it proved possible to recruit precisely such a team. The slots identified above were filled by:

(a) ***Dr Bob Nowill***, an independent security consultant who was Director of Cyber and Assurance at BT until 2013 and, prior to 2005, Director of Technology and Engineering at GCHQ;[42]

(b) ***Gordon Meldrum QPM***, Director of Intelligence at the National Crime Agency **[NCA]** until 2015, an experienced and demanding user of SIA intelligence product, particularly in the context of organised crime; and

(c) ***Cathryn McGahey QC***, a barrister with experience of criminal and civil cases and major inquiries who, as a special advocate acting in the interests of suspected individuals, had developed particular expertise in interrogating intelligence-based cases put forward by Government in the national security context.

A fuller description of the experience and expertise of each team member was given on my website when the Review was announced on 7 June.[43]

Contact with SIAs

1.33. I wrote personally to the three Agency chiefs at the outset of the Review to emphasise to them the need for the fullest disclosure and cooperation, to a very challenging time scale, if they were to do themselves justice in terms of persuading me of their case. All three SIAs responded with speed and efficiency.

---

[42] Dr. Nowill also acted as technical consultant to AQOT, as I recorded at AQOT 1.23. I have appreciated both his former detailed knowledge of GCHQ's secret systems (a rare commodity, without which it would not have been possible to interrogate and challenge GCHQ on a technically-informed basis) and his independent turn of mind, reinforced by a wealth of experience outside GCHQ.

[43] https://terrorismlegislationreviewer.independent.gov.uk/bulk-powers-review/.

1.34. The Review team has had access to all the closed material presented by the SIAs to the IPT and the ISC, including the records of closed evidence sessions. We also sought and obtained disclosure of extensive further material from all three SIAs, including contemporaneous intelligence reports and internal documentation relating to the utility (and relative utility) of SIA powers.

1.35. Three members of the Review team spent an introductory half-day at MI5, and Dr Nowill spent a half-day at GCHQ observing recent developments in technical capabilities and questioning GCHQ technical staff about them. The full team then spent a day at MI5, a day at MI6 and two days at GCHQ. In addition, members of the team, individually or in pairs, had further sessions with each of the SIAs in which specific technical matters were discussed and further explanations provided by the SIAs. There has been frequent further contact to follow up on specific points.

1.36. During the sessions attended by all four team members, managers and analysts from each SIA gave presentations during which they explained the uses to which bulk powers were put (or to which it was wished to put them), and provided examples in the form of case studies. Review team members were shown contemporaneous underlying documentation in respect of many of the case studies, requested further documentation, and had the opportunity to question those who had been involved in the cases about their decisions, the outcomes and possible alternative ways in which they might have been achieved.

1.37. At MI5 and GCHQ, all team members attended practical demonstrations of the use of bulk powers. The team was shown electronic records of previous operations, watched analysts at work on current operations and questioned them closely in relation to the capabilities they were using and their decision-making processes. Cathryn McGahey QC returned to MI6 to conduct a similar exercise there.

1.38. Following the initial meeting at GCHQ, Bob Nowill and Gordon Meldrum made a further visit in order to examine more deeply the use of bulk data by GCHQ, by reference to specific examples. They were shown all the material that they asked to see, witnessed demonstrations and held discussions at working level with operational staff. One case that they studied concerned the use of bulk interception and EI in cyber-defence, and the other the use of EI against overseas-based counter-terrorism targets.

1.39. We were mindful that EI (particularly at scale) is the newest and most rapidly-developing of the powers under review. It seemed to us inevitable that as with any new technology, teething troubles and wrong turns were bound to be experienced. Accordingly the full team, and subsequently Bob Nowill and Gordon Meldrum, took the opportunity to raise with GCHQ staff a number of

points made to us by NGOs, technical experts and others listed at 1.51-1.53 below about the unintended consequences of the use of EI, its cost-effectiveness, and the incidence of failed or unproductive operations. See further 2.68(b) and 7.24-7.25 below.

1.40. The human resources devoted to our visits to the SIAs, and to servicing our requests, were as follows:

(a) During the team's principal visit to MI5 we met with 19 MI5 officers; 52 were involved in planning and preparing the visit, and by early July MI5 had devoted more than 800 person hours to supporting the Review.

(b) During the team's principal visit to MI6 we met with 11 people; around 30 were involved in planning and preparing the visit, and by early July MI6 had spent around 130 person hours on preparation for and participation in the Review. These lower figures reflect the fact that, aside from BPDs, MI6 currently relies on the other SIAs' use of the bulk powers under review to support its operations.

(c) During the team's principal visit to GCHQ we met with 55 people, including military officers and integrees from other parts of Government. At least a further 75 staff were involved in planning and preparing the visit, and by early July GCHQ had devoted more than 1340 hours to supporting the Review.

Significant further resources were devoted to the Review by all three SIAs between early July and early August.

1.41. Those figures give some idea of the importance that the SIAs attached to this Review, and the effort that they put into servicing it. They are also a reminder that effective oversight brings with it costs in terms of staff time, including the time of senior management, front-line analysts and desk officers.

1.42. Separately, I contacted and spoke with the Ethics Counsellor at GCHQ, and with the Chair of one of the two Scientific Advisory Councils **[SACs]**, external committees of independent academics and industry experts that advise, respectively, GCHQ and MI5/MI6.[44]

Contact with users of SIA intelligence

1.43. It soon became apparent that even relatively sophisticated users of intelligence provided by the SIAs tend not to know much about the techniques by which it was obtained. For that reason, I concluded that there was little additional value

[44] The existence of the SACs has not previously been public knowledge. They were avowed at my request and with the consent of their respective Chairs (who, however, do not wish their own identities to be made public). See further 9.30 below.

to be gained from contacts with the Crown Prosecution Service **[CPS]** and with prosecuting counsel in terrorism and serious crime cases. I did however benefit from discussions with Helen Ball, the Police National Coordinator for Counter-Terrorism, and with Lynne Owens, Director General of the NCA, both of whom have knowledge and experience of the value to their operations of bulk intelligence obtained by the SIAs.

Contact with oversight bodies

1.44. As detailed in chapter 3 below, the exercise of some or all of the powers under review has already been considered in depth by a number of bodies and individuals with access to classified information. Those are the Investigatory Powers Tribunal, the Intelligence and Security Committee of Parliament, the Interception of Communications Commissioner and the Intelligence Services Commissioner **[IsComm]**.

1.45. I have read everything that those bodies and individuals have written about the powers under review, including material that was redacted from published reports of the ISC and contained in classified annexes to the reports of the Commissioners. The Review team has also read a large quantity of evidence submitted to the IPT (both open and closed), and written and oral evidence submitted by the SIAs to the ISC.

1.46. I also contacted and spoke to the President of the IPT (Sir Michael Burton, a Judge of the High Court) and Jonathan Glasson QC who has acted in relevant respects as counsel to the IPT; to the Chair of the ISC (Rt Hon. Dominic Grieve QC MP) and members of its staff; to the Head of the Office of the Interception of Communications Commissioner (Joanna Cavan OBE); to the Intelligence Services Commissioner (Sir Mark Waller, a retired Lord Justice of Appeal); and to the Head of his Office (Susan Cobb).

1.47. The Privacy and Civil Liberties Oversight Board **[PCLOB]** is a body of five lawyers, with technical assistance, which has in the recent past been charged with reviewing the utility of two capabilities which are said to have similarities with bulk powers in the Bill. The conclusions of one of those reports have been much relied upon by NGOs and parliamentarians who are sceptical of the utility of the powers under review. I first made contact with members of the PCLOB in 2014 during the preparation of AQOT, and have been particularly grateful during the Review for help from Jim Dempsey, one of its members, in explaining the background to its reports and subsequent developments.

Contact with NGOs and individuals

1.48. Critics of the powers under review who have not had access to classified evidence and information about their operation labour, through no fault of their own, under a significant disadvantage. Though the position was somewhat improved by the publication on 1 March 2016 of the Government's Operational Case, the examples and case studies there given are expressed at a relatively high level of generality. That point was strongly (and in my view, correctly) made by those who sought to address the claims made in that document: notably Liberty and Eric King (1.51 below).

1.49. It was however plainly important for the Review to have regard to the views of persons who have never enjoyed security clearance or had any connection with the activities of the SIAs.

1.50. A useful starting point was the voluminous evidence recently placed before the seven committees which considered the need for legislation, the draft Bill and the Bill itself. The team reviewed the evidence relevant to the subject matter of the Review. In view of its recent date, I did not issue a further general call for evidence.

1.51. I did however establish early contact (through its Director Eric King, and subsequently through Jim Killock) with the Don't Spy on Us Coalition **[DSOU]**, a coalition of the most influential organisations defending privacy, free expression and digital rights in Britain and Europe.[45] I received helpful advice and input from members and associated individuals, including advice on the structure of the Review and persons to contact. I am particularly grateful to Lord Strasburger and Peter Sommer for ideas on the structure of the Review, to Liberty for a detailed written submission of 31 July 2016,[46] to Michael Drury of BCL Burton Copeland solicitors and to a technically-minded lawyer who wishes to remain anonymous, for assisting my understanding of the range of purposes for which the powers under review could (notionally at least) be used.

Contact with technical experts

1.52. In a piece on my website announcing the launch of the Review, I also indicated a wish to speak to "*experts who, though without access to classified material, may*

[45] The Executive Committee of DSOU consists of Article 19, Liberty, Big Brother Watch, Open Rights Group, English Pen and Privacy International. Affiliates are Open Democracy, Public Concern at Work, Amnesty International, Access Now, Electronic Frontier Foundation, IFEX, XIndex, Centre for Investigative Journalism, Fight for the Future, World Wide Web Foundation, Open Media and Sum of Us.

[46] Liberty's written submission to the Review of 31 July 2016 is at https://www.liberty-human-rights.org.uk/sites/default/files/campaigns/resources/Liberty%27s%20submission%20to%20the%20Terrorism%20Reviewer%27s%20Review%20of%20Bulk%20Powers.pdf.

be able to inform our interrogation and scrutiny".[47] To that end, the Review team sought out and obtained useful input from Dr. Richard Clayton of the University of Cambridge and Dr. Paul Bernal of the University of East Anglia, who in addition to his academic responsibilities is a member of the recently-established Independent Digital Ethics Panel for Policing **[IDEPP]**.

1.53. I also used my website and social media to invite contact from anyone with specialist expertise or experience that could usefully assist the Review. In response, the Review had approaches from a number of people who had worked in a classified environment (including, in some cases, for an SIA) but who had subsequently moved out of that world. These people were of particular interest to the Review, because they combined an understanding of how the powers or similar powers had been used with an insight into how they are perceived by CSPs, internet service providers and others. Most (though not all) believed the powers under review to have at least some utility, but each brought insights of a technical and/or legal nature and, in some cases, suggestions for improvement. I am grateful in this respect for productive dialogues with John Davies, David Wells, Matt Tait, Gail Kent and Neil Brown (also a member of IDEPP) and with others who wished to remain anonymous, and for correspondence from the former NSA technical director, William Binney. The Review also received a short submission on behalf of five US tech companies, Facebook, Google, Microsoft, Twitter and Yahoo, which reiterated their view that "*governments should limit surveillance to specific, known users for lawful purposes, and should not undertake bulk collection of internet communications*".

1.54. The Review team had the opportunity to put to the SIAs for their comment many of the points made by the above persons, and to evaluate their written and oral responses.

Views of others

1.55. It goes without saying that none of those who made submissions or with whom the Review team had contact should be assumed to subscribe to the views expressed in this Report. In common with any factual errors, any views expressed are my responsibility alone. But having seen a final draft of this Report, each member of the Review team has asked me to say that they are fully in agreement with my conclusions and recommendation.

Completion of the Review

1.56. As is my usual practice, I have expressed my conclusions in a single open document from which no passages have been redacted. This means that it has

[47] https://terrorismlegislationreviewer.independent.gov.uk/bulk-powers-review/.

been possible to give only a flavour of the detailed classified material that has led me to those conclusions. Nonetheless, I believe that this Report constitutes the fullest assessment of the powers under review that has been published to date.

1.57. This report contains a number of matters that it was not open to me to disclose at the time of AQOT.[48] But effective intelligence work relies on its targets being uncertain as to precisely how such powers are used. There are dangers, including to the safety of the population, in disclosing sensitive tradecraft.

1.58. The requirement in RIPA 2000 s19 to keep secret many matters relating to interception warrants has further limited what can be said publicly, including in case studies.[49] This has not always deterred those seeking to relate the case studies to actual events.[50] I have pressed SIAs and others for the fullest possible public disclosure of sensitive material. But like others who have reviewed the current and anticipated future operational utility of sensitive intelligence techniques, I have had to acknowledge the often frustrating reality that there are limits to what I can explain or clarify in a public document.

1.59. In accordance with my terms of reference, this report has been submitted for fact and security checking prior to publication. Some relatively minor changes were called for as a consequence of that process, whose purpose is to minimise inaccuracy and ensure that no inadvertent disclosures are made of a kind that could damage national security. No pressure was exerted on me to alter any views expressed in this Report, and any attempt to do so would have been rejected without hesitation.

1.60. The Review's terms of reference give me the option of producing a classified annex to this report, for the benefit of the Prime Minister and the ISC. I was tempted: the Review team's consideration of case studies in particular occupied more time and effort than is apparent from the abbreviated summaries that I have been constrained to give in this Report.[51] But the purpose of this Report is to inform the parliamentary and public debate on the Bill. Its conclusions faithfully reflect my assessment of all the evidence I have seen. I concluded that there would be little to be gained by the production of an annex that could not be read by the intended audience for this Report.

---

48 Just as AQOT included material (e.g. its Annex 9) to which previous reports, including the 2015 ISC Report, had been unable to refer.

49 Clauses 54 and 123 of the Bill contain similar prohibitions.

50 See, e.g., Sean O'Neill, "GCHQ data harvesting led to drone strike on 7/7 chief", The Times, 13 June 2015, in which he sought to decode the case studies in AQOT Annex 9.

51 Chapters 5-8 and Annexes 8-11 below.

2. POWERS UNDER REVIEW

2.1. The purpose of this chapter is not to attempt any appraisal of the utility or necessity of the powers under review, but rather to identify those powers, to describe them briefly, to point the reader to more detailed descriptions elsewhere, and to summarise the nature of the controversy that they have attracted.

2.2. Past comments on the utility and necessity of the powers under review, and similar powers, are summarised in chapter 3 below.

2.3. It may be useful to record in tabular form the salient characteristics of each of the powers under review: whether they are unique to the SIAs; whether their use must be foreign-focused; whether they allow content as well as other data to be collected; whether they can be used for the purposes of preventing or detecting serious crime, even in the absence of a parallel national security purpose;[52] and which of the three SIAs (MI5, MI6 and GCHQ) uses or is expected to use the power provided for in the Bill.

Bulk power	Interception	Acquisition	EI	BPD
SIAs only?	YES	YES	YES	NO[53]
Foreign-focused?	YES	NO	YES	NO
Content included?	YES	NO	YES	YES
National security purpose required?	YES	YES	YES	NO
Power used by?	GCHQ	MI5, GCHQ	GCHQ	ALL

Powers not reviewed

2.4. The terms of reference for the Review (Annex 2), which were decided upon by the Government, make it clear that the Review does not extend to the whole range of powers in the Bill.

2.5. Nor, even, does the Review cover the whole range of powers that could be described as bulk powers in the broader sense of that phrase (1.5-1.6 above). Powers in the Bill which are liable to result in the collection or retention of large

[52] None of the powers under review may be used for the investigation or prosecution of ordinary (non-serious) crime.

[53] Though BPDs are retained and used also by non-SIAs such as the police, that activity (perhaps incongruously) does not fall within the scope of the Bill.

quantities of data not relating to current targets, but which fall outside the scope of this Review, are in particular:

(a) the power currently exercised under DRIPA 2014 to require CSPs to retain phone and email records, for the use (principally) of police **[the DRIPA power]**;[54]

(b) the proposed new power to require the retention of ICRs **[the ICR power]**;[55]

(c) the power to "*target*" an interception warrant on multiple persons or organisations who "*carry on, or may carry on, a particular activity*" or "*for the purposes of a single investigation or operation*", without necessarily knowing all their identities **[the thematic interception power]**;[56] and

(d) the power to "*target*" equipment interference on equipment "*in a particular location*", equipment that "*may be being used, for the purpose of a particular activity or activities of a particular description*" and so on **[the thematic EI power]**.[57]

It will be necessary to return to some of those powers for the purposes of assessing, in chapters 5-8, whether the objectives of the powers under review could be met as effectively by the use of other capabilities.

(1) Bulk Interception

Nature of bulk interception

2.6. The first power under review is the bulk interception of communications, which can be dated back to the interception of messages carried on the international cable system during the First World War.[58] The power is currently provided for (obscurely) in RIPA 2000 s 8(4),[59] and will in future be exercised under the bulk interception warrants provided for in Part 6 Chapter 1 of the Bill.

2.7. In the words of the open Operational Case (7.1):

> "Bulk interception is a capability designed to obtain foreign-focused intelligence and identify individuals, groups and organisations overseas that pose a threat to the UK. It allows the security and intelligence agencies to intercept the communications of individuals outside the UK and then filter and

54 Part 4 of the Bill; 2.33 below.
55 Clauses 59(6) and 83(9). As noted above, ICRs are a type of communications data.
56 Part 2 of the Bill, clause 17(2).
57 Part 5 of the Bill, clause 95.
58 It is claimed that bulk access to that commercially operated system enabled the collection of the Zimmerman telegram, the final trigger for US entry into the First World War, and detected attempts to evade the UK's economic blockade of Germany.
59 See further AQOT 6.45-6.59.

analyse that material in order to identify communications of intelligence value."[60]

2.8. A bulk interception warrant under the Bill will allow interception principally focused on "*overseas-related communications*" [61] in the course of transmission, the obtaining of "*secondary data*" [62] relating to intercepted communications, the selection for examination as described in the warrant of intercepted content or secondary data, and its disclosure.

2.9. The less intrusive option is also available of a bulk interception warrant that authorises the obtaining of secondary data only (clause 127(2)(b)).[63]

Thematic v bulk interception

2.10. It is clear from the Bill (clause 17) that a targeted interception warrant need not relate only to a single person or set of premises, but may relate also to

> *"a group of persons who share a common purpose or who carry on, or may carry on, a particular activity*"

and to

> "*more than one person or organisation, or more than one set of premises, where the conduct authorised or required by the warrant is for the purposes of a single investigation or operation*".

The thematic interception power, as it was referred to at 2.5(c) above, is thus a broad one.

2.11. The draft Code of Practice notes that "*There is not a limit to the number of locations, persons or organisations that can be provided for by a thematic warrant*", and that "*the warrant does not have to identify the subjects of the warrant any more than is possible at the time of the issue of the warrant*".

2.12. The potential scope of the thematic interception power is not as strikingly broad as that of the thematic EI power, and there is no equivalent section to 8.5-8.8 of the Operational Case, in which the Government warns that targeted thematic EI

---

60 See, further, the Interception of Communications draft Code of Practice, laid before Parliament when the Bill was introduced on 1 March 2016.

61 These are defined as communications sent or received by individuals who are outside the British Islands: clause 127(3).

62 ***Secondary data*** and ***equipment data*** are non-content data obtained under interception warrants and equipment interference warrants respectively. Both categories (which are very similar) comprise ***systems data***, which enables or otherwise facilitates the functioning of any system or service provided by the system (and which includes the communications data that can be obtained by means of a communications data authorisation), and ***identifying data*** which is capable of being logically separated from the rest of the communication or item of information.

63 As advised in AQOT, Recommendation 42(b).

can take place "*at scale*" and "*cover a large geographic area*". Nonetheless, it is true of these warrants as it is of their EI equivalents that they have some of the potential range of bulk warrants but without the same safeguards: the comments at 2.52-2.58 below are therefore of relevance here also.

How bulk interception works

2.13. Interception is the process of collecting communications in the course of transit, such that the content becomes available to someone other than the sender or recipient. The fruits of interception (the main focus of which must be overseas-related: clause 129(2)) can include both the content of such communications and information about them. Bulk interception typically involves the collecting of communications as they transit particular bearers (communication links).[64]

2.14. Bulk interception involves three stages, which may be called ***collection***, ***filtering*** and ***selection for examination***.[65]

First stage: collection

2.15. GCHQ selects which bearers to access based on an assessment of the likely intelligence value of the communications they are carrying. GCHQ does not have the capacity, or legal authority, to access every bearer in the world. Instead it focuses its resources on those links that it assesses will be the most valuable. At any given time, GCHQ has access to only a tiny fraction of all the bearers in the world.

Second stage: filtering

2.16. GCHQ's processing systems operate on the bearers which it has chosen to access. A degree of filtering is then applied to the traffic on these bearers, designed to select communications of potential intelligence value while discarding those least likely to be of intelligence value. As a result of this filtering stage, the processing systems automatically discard a significant proportion of the communications on the targeted bearers.

Third stage: selection for examination

2.17. The remaining communications are then subjected to the application of queries, both simple and complex, to draw out communications of intelligence value. Examples of a simple query are searches against a "*strong selector*" such as a

64 Bearers are explained in the 2015 ISC Report, p.26 at fn 48. There were then c. 100,000 bearers joining up the global internet. The ISC gave the example of 47 separate 10 gigabit per second bearers carried in a single transatlantic cable, but noted that the capacity of both bearers and cables is expanding fast as technology develops.

65 Further information is given (I believe accurately, though with many redactions from the open version) in the 2015 ISC Report, para 49-77.

telephone number or email address. Complex queries combine a number of criteria, which may include weaker selectors but which in combination aim to reduce the odds of a false positive. Communications that match the chosen criteria are automatically retained, and all other communications are automatically discarded. The retained communications are available to analysts for possible examination.

2.18. The application of these queries may still leave too many items for analysts to examine, so GCHQ must then carry out a triage process to determine which will be of most use. This triage process means that the vast majority of all the items collected are never looked at by analysts. Even where communications are known to relate to specific targets, GCHQ does not have the resources to examine them all. Analysts use their experience and judgement to decide which of the results returned by their queries are most likely to be of intelligence value and will examine only these.

The two major processes

2.19. A description is given in the 2015 ISC report (paras 61-73), of two major and distinct processes that apply to interception under bulk warrants. Those processes are identified in more detail in the closed version of the report, and I have been briefed on each of them. In summary:

(a) ***The "strong selector" process*** (2015 ISC report, paras 61-64) operates on the bearers that GCHQ has chosen to access. As the internet traffic flows along those chosen bearers, the system compares the communications against a list of strong selectors in near real-time. Any communications which match the selectors are automatically collected and all other communications are automatically discarded. The nature of the global internet means that the route a particular communication will take cannot be predicted and a single communication is broken down into packets which can take different routes. In order to identify and reconstruct the wanted communications of subjects of intelligence interest, GCHQ's processing relies on accessing the "*related communications data*" (secondary data) in the bearer.

A copy of all the communications on a bearer has to be held for a short period in order to allow the strong selectors to be applied to those communications. This process accordingly requires a bulk warrant under the Bill. However, in the opinion of the ISC, "*while this process has been described as bulk interception because of the numbers of communications it*

covers, it is nevertheless targeted since the selectors used relate to individual targets".[66]

(b) ***The "complex query" process*** (2015 ISC report paras 65-73) is used where GCHQ is looking to match much more complicated criteria, for example with three or four elements. This process operates across a far smaller number of bearers. These bearers are not chosen at random, as GCHQ focuses its resources on those most likely to carry communications of intelligence value. As a first step in the processing under this method the system applies an initial set of processing rules. Those rules seek to select communications of potential intelligence value while discarding those least likely to be of intelligence value. The selected communications are not available to GCHQ staff to search through at will. Further complex searches draw out the communications of intelligence value. By performing searches combining a number of criteria, the odds of a 'false positive' are considerably reduced.

This second process is closer to true bulk interception, since it involves the collection of unselected content and/or secondary data. It permits types of analysis and selection that are not currently achievable in the near real-time environment of the strong selector process (2.19(a) above). But as with the first process, it remains the case that communications unlikely to be of intelligence value are discarded as soon as that becomes apparent.

2.20. The ISC March 2015 Report rejected allegations of untargeted or blanket surveillance, concluding at para 64 that:

> "This interception process does not therefore collect communications indiscriminately"

and at para 77 that:

> "Only the communications of suspected criminals or national security targets are deliberately selected for examination."

I have no reason to disagree with those assessments, though it is outside the scope of my functions and of this Review to conduct a detailed examination of GCHQ's collection and selection processes. Such examinations are conducted by technically skilled inspectors in the IOCC's Office **[IOCCO]** (see 3.5(a) below) and will in future be conducted by the IPC.

---

[66] 2015 ISC Report, para 64. The analogous power in the USA was described as a targeted power by the PCLOB: 3.53(b) below. Liberty, in its submission to the Review of 31 July 2016 (para 17), refers to the product of filtering which relates to targets – as is, in practice, it always does - as "*a rich store of **targeted** data*". It is not clear therefore that Liberty actually objects to GCHQ's use of the strong selector process, despite the fact that for the purposes of the Bill it is classed as a bulk interception capability. This affects Liberty's analysis e.g. at para 42.

Product of bulk interception

2.21. It is GCHQ's ability to interrogate the data obtained through bulk interception that has been retained following the selection for examination stage (2.17-2.18 above) that provides the capability to answer questions about developing incidents as they occur and identify the individuals involved. Much of the information needed to produce this intelligence is drawn from a composite of individual pieces of data, some of them long pre-dating the event.

2.22. The 2015 ISC Report made the point (para 80) that the value of bulk interception lies not just in the "*actual content of communications*" but in "*the information associated with those communications*", including both:

(a) communications data, "*limited to the basic 'who, when and where'"; and*

(b) content-derived information, "*including the characteristics of the communication*".[67]

The ISC added that to its own surprise, the primary value to GCHQ of bulk interception lay not in the content but in the associated information.

2.23. The Bill applies a slightly different set of definitions. Bulk interception may produce the following categories of data:

(a) ***Content***, defined in clause 233(6) in terms of the meaning of any communication; and.

(b) ***Secondary data*** (similar to what the ISC called communications data, and informally known as ***metadata***), defined in clause 128 by reference to

- ***systems data***, defined in clause 235(4) and (5) as including data that enables or facilitates the functioning of a telecommunication system or service; and
- ***identifying data*** defined in clause 235(2)(3) as including data that identifies a person, apparatus, system, service, event or location[68]

that meet the qualifying conditions set out in s128(4)(5).

As noted at 2.9 above, a bulk interception warrant may be limited to secondary data.[69]

---

67 This is currently referred to by GCHQ as Content-Derived Metadata, and distinguished by them both from communications data and from "*true*" content.

68 Identifying data must however be logically separable from the content of a communication, or private information: thus, I am told that it is not understood by the SIAs to cover, for example, a linguist's conclusion that a speaker has a particular regional accent.

2.24. Even so-called "*secondary data*" can enable the tracing of contacts, associations, habits and preferences. It has been said to encompass "*location data that can be used to track people's movements, login passwords, and website browsing histories".*[70] Analysis of secondary data collected in bulk may provide the critical information required to open the way to individual requests, e.g. targeted interception or targeted EI. But secondary data also encompasses the highly technical non-personal information that GCHQ told the Review was crucial for them to understand global telecommunications infrastructure. That includes, for example, information about protocols and server routing.

Safeguards on bulk interception

2.25. The internal safeguards applicable to the retention, storage and destruction of intercepted material and related communications data were examined in detail by IOCCO in its report for 2013.[71] The Commissioner's findings included that:

(a) in relation to content, "*indiscriminate retention for long periods of unselected intercepted material (content) does not occur*" (para 3.55); and

(b) in relation to communications data, that he remained to be satisfied that some of the "*variety of longer periods*" for which it was retained could be justified (para 3.56).

Major reviews of retention, storage and destruction procedures ensued, and all 33 of the specific recommendations made by the IOCC in 2013 and 2014 were accepted.[72]

2.26. The external safeguards in the Bill applicable to bulk interception warrants are set out in the draft Code of Practice[73] and summarised at paras 7.6-7.15 of the Operational Case. In brief and non-exhaustive outline:

(a) Warrants must be signed and issued personally by the Secretary of State (clause 132), with the approval of a Judicial Commissioner (clause 131). Application must be made by an SIA Head (clause 129(1)).

(b) The Secretary of State (and the Judicial Commissioner in exercising his function of review) must consider that the warrant is necessary in the interests of national security (whether on its own or in conjunction with other

---

69 Clause 127(4).

70 Ryan Gallagher, The Intercept, 7 June 2016: "*Facing data deluge, secret UK spying report warned of intelligence failure*": https://theintercept.com/2016/06/07/mi5-gchq-digint-surveillance-data-deluge/.

71 2013 Annual Report of the Interception of Communications Commissioner, April 2014, 3.48-3.57.

72 2014 Report of the Interception of Communications Commissioner, March 2015, 6.60-6.65.

73 Interception of Communications draft Code of Practice, March 2016, chapter 9.

grounds, including the prevention and detection of serious crime: clause 129(1)(b)).

(c) They must further consider that examination of intercepted content or secondary data obtained under the warrant is or may be necessary for the Operational Purposes specified in the warrant, and proportionate (clause 129(1)(c)(d)).

(d) They must have regard to factors including whether less intrusive means could be used, the integrity and security of telecommunications system and the protection of privacy (clause 2; see also clauses 129 and 130).

(e) Despite the foreign focus required by clause 127(2)(3), bulk interception (e.g. of the contents of an international cable) will inevitably collect communications between persons in the UK, for example via a server outside the UK. A targeted examination warrant, with the further safeguards provided for under Part 2 of the Bill is required before it is possible to select for examination the content of the communications of a person known to be in the UK (clause 15(3)).

(f) Further safeguards (detailed in the draft Code of Practice, and now on the face of the Bill) apply to the retention, disclosure, examination and destruction of data obtained by bulk interception and to items subject to legal professional privilege **[LPP]** (clauses 140-143).

(g) The operation of current bulk interception powers is subject to the audit of IOCCO, including its technical inspectorate, and will in future be audited by the IPC. The 2015 ISC Report recommended that the oversight body be given express authority to review the selection of bearers, the application of simple selectors and initial search criteria, and the complex searches which determine which communications are read.[74] That authority is (I am assured by the Home Office) inherent in clauses 205 and 211 of the Bill.[75]

Criticisms of bulk interception

2.27. A flavour of the criticisms of bulk interception, as they have previously been communicated to me, was given in AQOT 12.35-12.42. In particular:

[74] 2015 ISC Report, paras 123-125.

[75] See, in particular, the clause 205(5) duty on the IPC to "*keep under review the operation of safeguards to protect privacy*".

(a) It is maintained that the privacy of the individual is intruded into not only when material is read, analysed and shared with other authorities, but also when it is collected, stored and filtered without human intervention.[76]

(b) The mere knowledge that the state has the ability to collect such material (whether or not it is accessed) is said to give the state the whip hand over the individual, and to suppress individual autonomy.

(c) There are concerns about the risk of abuse and unauthorised access that are posed by holding vast quantities of data, particularly content, in one place.

(d) It is said not only that bulk interception is disproportionate, but that it is impossible to have a meaningful assessment of proportionality at that level.

(e) It is suggested that bulk collection systems are not capable of providing sufficient protection for material covered by LPP, material relating to journalists and so on.[77]

2.28. More fundamentally, it has been suggested on the basis of CJEU case law that *any* bulk collection of the content of communications is *per se* unlawful.[78]

(2) Bulk Acquisition

Nature of bulk acquisition

2.29. The second power under review is bulk acquisition, currently practised under TA 1984 s94, and provided for in Part 6 Chapter 2 of the Bill. Until the draft Bill was published on 4 November 2015, the existence of the capability was an extremely tightly-controlled secret.[79]

2.30. Section 94 empowers the Secretary of State to give providers of public telecommunications networks:

---

[76] That is indeed the legal position. The UK's Supreme Court, applying the law as declared by the ECtHR, declared in 2015 that "*the state's systematic collection and storage in retrievable form even of public information about an individual is an interference with private life*": *Catt v MPC* per Lord Sumption at para 6. The position in the US is less clear.

[77] A detailed critique is contained in the witness statements of Eric King in *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and others*, Case No. IPT/13/92/CH.

[78] In Case C-362/14 *Schrems v Data Commissioner* ECLI:EU:C:2015:650, para 94, the CJEU commented that "*legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life* ...". The bulk interception regime does allow for the collection of content in bulk, though the Government may be expected to argue, if necessary, that access to that content is not granted on a generalised basis, and that the distinction suggested by the CJEU is hardly a binary one, given that content is held for only a few seconds under the procedure outlined at 2.19(a) above.

[79] Though Gordon Corera, the BBC's Security Correspondent, referred to the use of s94 directions for this purpose as "*likely*" in his book *Intercept: the secret history of computers and spies* (Weidenfeld & Nicolson, June 2015), chapter 17 fn 6.

".. *such directions of a general character as appear to the Secretary of State to be necessary in the interests of national security or relations with the government of a country or territory outside the United Kingdom*".

The generality of that provision is further underlined by the fact that there is (and is proposed to be) no statutory definition of national security.

2.31. Part 6 Chapter 2 of the Bill provides a more precise statutory basis for the capability. It gives the Secretary of State, on the application of the Head of an Agency and after approval by a Judicial Commissioner, the power to issue a bulk acquisition warrant. Such a warrant cannot apply to the content of communications, but may require a telecommunications operator to retain communications data and to disclose it to a person specified in the warrant.

2.32. In contrast to bulk interception and bulk EI (but like BPDs), there is no requirement for bulk acquisition to be foreign-focused. The "*who, when and where*" of domestic communications such as phone calls and emails (though not their content) may therefore legitimately be the intended focus for collection under the power.

2.33. Another important and distinctive feature of the current capability is that data obtained pursuant to it can be aggregated in one place. That distinguishes it from the data retention powers that have been provided for successively by Regulations under the Data Retention Directive,[80] by the DRIPA power,[81] and now by Part 4 of the Bill. The existence of an aggregated database (as opposed to the federated databases kept by each CSP subject to standard data retention obligations) is said to be a key element in the added value of the bulk acquisition power.

2.34. I was told that the aggregated database which is enabled through the bulk acquisition power is likely to retain advantages even after such time as the filtering arrangements provided for in the Bill for interrogating multiple databases (clauses 63-65) may have been designed and developed.[82] This will plainly have to be kept under review, since it is at least notionally possible that a search filter applicable to numerous databases could achieve similar results in a less intrusive manner.

---

80 Directive 2006/24/EC, which required service providers to retain data generated for billing purposes concerning the use of telephone, internet and email services for between six and 24 months, was declared invalid by the CJEU in Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland* ECLI:EU:C:2014:238. The UK implementing Regulations were replaced by the DRIPA power later in 2014.

81 See AQOT 6.60-6.70 and 2.5(a) above.

82 See 6.26-6.28 below.

How bulk acquisition works

2.35. Secret directions under s94 have since at least 2001 (GCHQ) and from 2005 (MI5) enabled the SIAs to acquire communications data in bulk, including in particular records of domestic communications, for the purposes there set out.

2.36. The first detailed open review of this activity was published on 7 July 2016 by the IOCC, who noted in his cover letter that a statutory requirement of secrecy:

> " severely limits what we can say publicly about the nature of the directions and the conduct undertaken in pursuance of any direction".

IOCCO also had to be mindful of the case which was then pending before the IPT, judgment in which is likely to be handed down in the coming months. [83]

2.37. Some useful detail of existing practice is however provided in the IOCCO Report. Each of the 15 extant s94 directions for bulk communications data were said (at 8.34) to require the disclosure of traffic data (which identifies e.g. the sender and recipient of a communication, the location from which and time at which it was sent and other related material).[84] The report dealt with the preparation of submissions for a s94 direction (8.37-8.44), the giving of a s94 direction (8.47-8.49), handling and storage arrangements (8.54-8.57), access to bulk communications data (8.58-8.70) and acquisition and access errors (8.71-8.83).

2.38. Looking forward to the implementation of the Bill, section 10 of the IOCCO report welcomed what it described as the "*clear requirements and safeguards*" set out in the Bill and in the 44-page Bulk Acquisition Draft Code of Practice.

2.39. The draft Code of Practice summarises matters as follows:

> "3.1 Bulk acquisition warrants authorise a two stage process. First, the obtaining of BCD [bulk CD] from a CSP and second, the selection for examination of the BCD obtained under the warrant.
>
> 3.2 A bulk acquisition warrant will be served on a CSP to require that CSP to disclose the communications data specified in the warrant. This may also require a CSP to obtain and disclose specified communications data that is not in its possession but that it is capable of obtaining.
>
> 3.3 A warrant will normally provide for the provision of communications data as it is generated or processed by the CSP for business purposes but may also relate to the provision in bulk of communications data retained by a CSP for business purposes or

---

83 *Privacy International v Secretary of State for Foreign and Commonwealth Affairs et al*, IPT/15/110/CH.

84 RIPA 2000 s21(4)(a).

under the provisions in Part 4 of the Act. This may result in the collection of large volumes of communications data. This is essential to enable communications relating to subjects of interest to be identified and subsequently pieced together in the course of an investigation.

3.4 In contrast to a targeted communications data authorisation, issued under Part 3 of the Act, a bulk acquisition warrant instrument need not be constrained to a specific operation.

3.5 Chapter 2 of Part 6 does not impose a limit on the volume of communications data which may be acquired. For example, if the requirements of this chapter are met then the acquisition of all communications data generated by a particular CSP could, in principle, be lawfully authorised but only where necessary and proportionate to do so. This reflects the fact that bulk acquisition is an intelligence gathering capability, whereas targeted communications data acquisition is primarily an investigative tool that is used to acquire data in relation to specific investigations.

3.6 Accordingly, and in contrast to targeted communications data acquisition, a warrant may only be sought by a member of the SIA. In addition, the volume of data which may potentially be acquired is reflected in that fact that bulk acquisition warrants must be granted by the Secretary of State and are subject to authorisation by the Judicial Commissioner. Once acquired in bulk, selection of data for examination is only permitted for approved operational purposes.

3.7 In contrast to the bulk powers provided for in Chapters 1 and 3 of Part 6 of the Act, a bulk acquisition warrant may relate to communications data in relation to individuals in the UK."

Further sections of the draft Code of Practice deal with the obtaining of warrants, modifications, renewals and cancellation, implementation of a technical capability, safeguards, record keeping and error reporting.

Product of bulk acquisition

2.40. I regret that I am unable openly to describe:

(a) the precise categories of communications data that are currently subject to s94 directions (though the IOCCO report has said that all concern traffic data);

(b) the specific purposes which those data currently serve, in the hands of MI5 and GCHQ, beyond stating that both use them for the full range of their statutory functions;

(c) the categories of data that it is envisaged will be subject to bulk acquisition warrants under the Bill; or

(d) the categories of CSP that may be in receipt of such directions or warrants.

2.41. It can safely be said however that:

(a) the existing power and the power in Part 6 Chapter 2 of the Bill both enable the SIAs to obtain large amounts of communications data, most of it relating to individuals who are unlikely to be of any intelligence interest; but that

(b) content cannot be obtained under either power, and it is not currently envisaged that the bulk acquisition power in the Bill will be used to obtain internet connection records.[85]

Safeguards on bulk acquisition

2.42. The safeguards applicable to bulk acquisition are similar to those which apply to bulk interception and bulk equipment interference, save that there is no requirement of a foreign focus. In particular:

(a) Warrants may be signed and issued personally by the Secretary of State (clause 148), with the approval of a Judicial Commissioner (clause 147), on the application of an SIA Chief (clause 146(1)).

(b) The Secretary of State (and the Judicial Commissioner in exercising his function of review) must consider that the warrant is necessary in the interests of national security (whether on its own or in conjunction with other grounds, including the prevention and detection of serious crime: clause 146(1)(a)).

(c) They must further be satisfied that the interrogation of data obtained under the warrant is or may be necessary for the Operational Purposes specified in the warrant, and proportionate (clause 146(1)(b)(c)).

(d) They must also have regard to factors including whether less intrusive means could be used, the integrity and security of telecommunications systems and the protection of privacy (clause 2).

(e) Further safeguards (contained so far as possible in a statutory Code of Practice) apply to the retention, disclosure, examination and destruction of data (clauses 158-159).

[85] A "Bulk Communications Data" factsheet published with the draft Bill on 4 November 2015 stated "*The data does not include internet connection records ...*". I am told however that this is no more than a statement of present practice and intention: neither the Bill nor the draft Code of Practice rules out the future use of the bulk acquisition power in relation to ICRs.

(f) Operation of the power is audited by IOCCO and will in future be audited by the IPC.

Criticism of bulk acquisition

2.43. In January 2016, not long after the existing bulk acquisition capability was avowed for the first time, Privacy International amended an existing claim in the IPT to challenge the use of TA 1984 s94, including for the purposes of bulk acquisition. It claimed, *inter alia*, that:

(a) the regime governing the acquisition, use, retention, disclosure, storage and deletion of private information under s94 was not sufficiently accessible to the public, and contained insufficient safeguards to provide proper protection against arbitrary conduct;

(b) the s94 regime was not necessary or proportionate; and that

(c) the effect of using s94 was to circumvent specific safeguards contained in other legislation.

Some of those arguments were specific to the legal regime currently in force, but others (particularly as relates to necessity and proportionality) might also have been applied to the legal regime in Part 1 Chapter 2 of the Bill.

2.44. The case was argued in July, by reference to disclosure given by the Government as to the use of s94, and judgment is expected in the coming months. I have reviewed the transcript of the hearing but say nothing more about the arguments, which will be authoritatively ruled upon by the IPT.

(3) Bulk Equipment Interference

Nature of bulk EI

2.45. The third power under review is bulk EI, provided for in Part 6 Chapter 3 of the Bill. EI covers a range of techniques involving interference with computers. Most of these techniques fall within the scope of what was previously known as computer network exploitation **[CNE]**. The most commonly understood of them include what may be colloquially referred to as hacking or the implantation of software into endpoint devices or network infrastructure to retrieve intelligence, but EI may also include, for example, copying data directly from a computer.

2.46. From the point of view of the authorities, EI has an important advantage over bulk interception. In the words of the IPT:

> "The particular significance of the use of CNE is that it addresses difficulties for the Intelligence Agencies caused by the ever increasing use of encryption by those whom the Agencies would wish to target for interception."[86]

2.47. EI can give the SIAs access to a wide range of material, including the content of communications as well as equipment data.[87] Such material may well, depending on the case, have been rendered impossible or very difficult to intercept by end-to-end encryption. EI thus represents one answer to the "*going dark*" problem to which I referred in AQOT 10.17-10.19, and of which I have seen further evidence during the course of this Review, including in internal SIA documents.

2.48. EI is currently practised pursuant to authorisations under ISA 1994 ss 5 (inside or outside the UK) and 7 (outside the UK): see AQOT 6.24-6.33 and 7.62-7.65. In the absence of such legal authorisation, most CNE operations would amount to offences under the Computer Misuse Act 1990.

2.49. Interference with property or wireless telegraphy that is not for the purpose of acquiring communications, equipment data or other information (for example, disabling an alarm system to obtain covert access to a building) is not EI and continues to fall within the definition of "*property interference*", governed by ISA 1994 ss 5 and 7 or Part 3 of the Police Act 1997.[88]

2.50. EI was avowed for the first time in February 2015, when the Government published a draft Equipment Interference Code in response to a case brought by Privacy International in the IPT.[89] A much more detailed draft Code of Practice, with specific provision for bulk EI, was published alongside the Bill in March 2016.

Thematic vs bulk EI

2.51. It is important to understand the difference between targeted EI and bulk EI, which because of the wide potential scope of the thematic EI power relates not so much to the possible scope of a warrant as to the applicable safeguards. In short summary:

(a) ***Targeted EI warrants*** (clause 93(2)) may be sought by an SIA Head but also by the Chief of Defence Intelligence and by a Law Enforcement Chief (e.g. the Chief Constable of a police force). There is no requirement for a

---

86 *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and GCHQ* [2016] UKIPTrib 14_85-CH, para 3.

87 Clause 93(2) (targeted EI) and clause 162(1)(b) (bulk EI).

88 *Ibid.*, 2.6-2.7.

89 For the link, see *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and GCHQ* [2016] UKIPTrib 14_85-CH, para 11.

link to the interests of national security: it is enough that the warrant be necessary for the purpose of preventing or detecting serious crime, or (in some cases) preventing or mitigating death, injury or damage to a person's physical or mental health. Nor is there any requirement that a targeted EI warrant be foreign-focused.

(b) ***Bulk EI warrants*** (clause 162) are more tightly controlled, in the manner of bulk interception warrants: they may be sought only by the SIAs; they must be necessary in the interests of national security (whether on its own or in conjunction with other grounds, including the prevention and detection of serious crime);[90] and a foreign focus is required. In the same way as for bulk interception, a targeted examination warrant (clause 93(9)) is required to carry out the selection for examination of the protected material of individuals known to be within the UK or the private information of such individuals.

2.52. Targeted EI warrants, used thematically, may be very broad in their scope: they may relate for example to "*equipment in a particular location*", "*equipment in more than one location, where the interference is for the purpose of a single investigation or operation*" and "*equipment which is being, or may be, used for the purposes of a particular activity or activities of a particular description*".[91]

2.53. The Government has expressly acknowledged that targeted thematic EI operations, like their bulk counterparts, can take place "*at scale*", and that they may cover a large geographic area or involve the collection of a large volume of data.[92] The Code of Practice specifies that "*the activity should be focused on specified targets as much as possible to ensure only so much product is obtained and examined as is necessary and proportionate.*"[93] Yet the thematic EI power is subject to fewer limitations. In particular, targeted thematic EI operations:

(a) can be conducted by a wider range of authorities (including the police),

(b) need not be connected with national security, and

(c) need not be overseas-focused.

2.54. I do not challenge the operational case for targeted thematic EI warrants, including within the UK where they may be useful to MI5 e.g.:

---

90 Clause 164(1)(b).

91 Clause 95(1)(d)(e)(f); compare clause 17(2) (targeted thematic interception warrants).

92 Operational Case, 8.5; see further March 2016 draft Code of Practice, 4.17.

93 March 2016 draft Code of Practice, 5.3; cf. the discussion of thematic warrants by the IPT in *Privacy International v Secretary of State for Foreign and Commonwealth Affairs* [2016] UKIPTrib_14 85-CH (12 February 2016), paras 31-47.

(a) where EI targeted on one subject of interest may impact on others who use the same device or are part of the same network;

(b) where covert entry is effected into a property, and it may be necessary and proportionate to interfere with all the devices in the premises because it is not immediately possible to identify which belong to the subject of interest;

(c) for the investigation of groups whose members are not in the same location and whose communications may not be visible through interception: factors such as speedy online radicalisation mean that MI5 may no longer be able to rely on more traditional surveillance methods in such cases; or

(d) to investigate cyber-attacks on networks in the UK..

2.55. I am mindful also of the ruling of the IPT that it is not necessary for an EI warrant to be limited to a named or identified individual or list of individuals: "*The property should be so defined, whether by reference to persons or a group or category of persons, that the extent of the reasonably foreseeable interference caused by the authorisation*" of the actions authorised by the warrant can be addressed.[94]

2.56. But I have previously commented that the widely-drawn provision for targeted thematic EI "*effectively imports an alternative means of performing bulk EI, with fewer safeguards*".[95] To the Government's answer that targeted thematic EI warrants will only be used in cases where the proposed interferences with privacy are adequately foreseeable, such that "*the additional access controls under the bulk EI warrantry regime are not required*",[96] I responded that this "*may be argued to place excessive weight on the discretion of decision-makers*", and suggested that it should be possible to "*reduce the scope of [targeted thematic warrants] so as to permit only such warrants as could safely be issued without the extra safeguards associated with bulk*".

2.57. That comment relates however to the desirable scope of targeted warrants under Part 5 of the Bill, and not to the powers under review. For that reason I do not pursue it in this report, save to note that it will be particularly important for those authorising and approving warrants to ensure that the thematic powers are kept within strict bounds, and not used as a means of avoiding or circumventing the restrictions that have quite properly been placed on the authorisation of bulk warrants. I hope and expect that the IPC will keep a particularly close eye on this.

---

94 *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and GCHQ* [2016] UKIPTrib 14_85-CH, para 38.

95 Written evidence of 24 March 2016 to Parliament's Public Bill Committee, para 5(a): http://www.publications.parliament.uk/pa/cm201516/cmpublic/investigatorypowers/Memo/IPB46.htm.

96 *Ibid.*, 8.6; March 2016 draft Code of Practice, 5.5.

How bulk EI works

2.58. In the words of the 2016 draft Code:

> "Equipment interference warrants authorise all actions necessary for the obtaining of communications, equipment data or other information from equipment.
>
> …
>
> Equipment interference can be carried out either remotely or by physically interacting with the equipment. At the lower end of the scale, an equipment interference agency may covertly download data from a subject's mobile device when it is left unattended, or an agency may use someone's login credentials to gain access to data held on a computer. More complex equipment interference operations may involve exploiting existing vulnerabilities in software in order to gain control of devices or networks to remotely extract material or monitor the user of the device."[97]

2.59. In a judgment of February 2016, the IPT recorded a number of avowals (or admissions) by the Government concerning the use of EI, then referred to as CNE, including the following:

(a) GCHQ carries out CNE within and outside the UK.

(b) In 2013 about 20% of GCHQ's intelligence reports contained information derived from CNE.

(c) GCHQ undertakes both "*persistent*" and "*non-persistent*" CNE operations, namely both where an implant expires at the end of a user's internet session and where it "*resides*" on a computer for an extended period.

(d) CNE operations undertaken by GCHQ can be against a specific device or a computer network.[98]

2.60. It was further agreed that CNE/EI *might* be used by GCHQ so as to involve the following:

(a) the obtaining of information from a particular device, server or network;

(b) the creation, modification or deletion of information on a device, server or network;

(c) the carrying out of intrusive surveillance;

---

97 Equipment Interference Draft Code of Practice, March 2016, 2.1, 2.4.

98 *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and GCHQ* [2016] UKIPTrib 14_85-CH, para 5.

(d) the use of CNE in such a way that it creates a particular security vulnerability in software or hardware, in a device or on a network;

(e) the use of CNE in respect of numerous devices, servers or networks, without having first identified any particular device or person as being of intelligence interest (referred to as bulk CNE);

(f) the use of CNE to weaken software or hardware at its source, prior to its deployment to users; and

(g) the obtaining of information for the purpose of maintaining or further developing the SIAs' CNE capabilities.[99]

In accordance with its usual practice, the IPT agreed to "*make assumptions as to the significant facts in favour of the Claimants*" and so to proceed on the basis that these practices could be assumed to be taking place, even though in many cases they had been met with an NCND response.[100]

2.61. The dividing line between large-scale targeted and bulk EI is not an exact one, but as already noted (1.19 above), GCHQ has not to date conducted any operations which would, under the Bill, be authorised by a bulk EI warrant.

Product of bulk EI

2.62. A bulk EI warrant may (by clause 162(1)) authorise interference with any equipment for the purpose of obtaining:

(a) ***communications*** (defined in clause 181);

(b) ***equipment data*** (defined in clause 163 in terms of ***systems data*** and ***identifying data*** that meets certain qualifying conditions);[101] and

(c) ***"any other information"***.

2.63. As previously noted, the main purpose of the warrant must be to obtain overseas-related communications, information or equipment data (clause 162(1)(c)), as defined in clause 162(2)-(3), though it is acknowledged that other material may well be obtained at the same time.

2.64. It should not however be assumed that bulk EI will invariably recover content. Indeed on the contrary, GCHQ told us that in the majority of cases the use of bulk EI will be designed to return equipment data with a view to identifying a

99 *Ibid.,* para 9. The limited extent to which those practices were avowed as actually taking place is recorded in that paragraph by the IPT.

100 *Ibid.*, para 2.

101 Compare the similar definition of secondary data in clause 128: 2.23(b) above.

limited number of devices in respect of which more intrusive techniques could then be deployed.

Safeguards on bulk EI

2.65. Similar safeguards to those applicable to bulk interception (2.26 above) apply to applications for bulk EI warrants and their authorisation, approval and modification. Together with the safeguards that apply to the selection for examination of content obtained under a bulk EI warrant, they are set out in the Bill and expanded upon in the draft Code of Practice.[102]

2.66. The operation of EI is subject to the oversight of the IsComm, and will be overseen by the IPC once the Bill becomes law.

Criticism of bulk EI

2.67. Though EI (then known as CNE) was only avowed in February 2015, the Snowden documents had suggested that it was being practised some years before that date, and many of the criticisms are based upon readings of those documents. Summarising the criticisms made by Privacy International and other groups in their challenge before the IPT, it was suggested that:

(a) The tools used by GCHQ allow vast quantities of historical and current information to be extracted from large numbers of devices, subjecting users to mass and intrusive surveillance. Eric King of Privacy International claimed:

> "CNE gives intelligence agencies access to the most personal and sensitive information about an individual's life – information which can directly or indirectly reveal an individual's location, age, gender, marital status, finances, health details, ethnicity, sexual orientation, education, family relationships, private communications and, potentially, their most intimate thoughts. Furthermore, the logging of keystrokes, tracking of locations, covert photography, and video recording of the user and those around them enables intelligence agencies to conduct real-time surveillance, while access to stored data enables analysis of a user's movements for a lengthy period prior to the search",

and described CNE as "*the most powerful and intrusive capability GCHQ possesses*". Examples followed of what malware can do against an individual device and against a server or network.[103]

---

[102] Clauses 162-180 of the Bill; March 2016 draft Code of Practice, sections 3 and 5. See also Operational Case at 8.9-8.18.

[103] Witness statement of Eric King of 5 October 2015, paras 10 and following: https://www.privacyinternational.org/sites/default/files/Witness_Statement_Of_Eric_King.pdf. .

(b) EI creates potential security vulnerabilities or leaves users vulnerable to further potentially grave damage.[104]

(c) Ministers lack sufficient understanding of the methods employed by GCHQ to enable them properly to assess necessity and proportionality when authorising warrants for EI.[105]

2.68. Having considered a great deal of closed material, including extensive disclosure, the IPT concluded that "*the use of CNE by GCHQ has obviously raised a number of serious questions*". Though it found no breach of the law in its judgment of February 2016, and ruled that "*in principle CNE is lawful*", it added that:

> "If information were obtained in bulk through the use of CNE, there might be circumstances in which an individual complainant might be able to mount a claim …".[106]

Privacy International has sought to take the case further, by way of a claim for judicial review before the Administrative Court in London and an application to the European Court of Human Rights.

(4) Bulk Personal Datasets

Nature of BPDs

2.69. The fourth and final power under review is the power of the SIAs to retain and use BPDs under Part 7 of the Bill. The recognition by the SIAs of the value of BPDs is said to date back to the early years of the century:[107] but the power was first disclosed in the 2015 ISC Report.[108]

2.70. In the words of the Operational Case (10.1):

Ciaran Martin of GCHQ, in his first open witness statement of 16 November, paras 36-37, denied that the system entitled GCHQ to conduct "*mass*" or "*bulk*" surveillance, and responded that "*a significant proportion of the examples given in the Claimants' evidence with respect to the possibilities created by CNE tools bear no relation to the reality of GCHQ's activity and/or would be unlawful having regard to the relevant statutory regime*".

104 Ciaran Martin, in his first witness statement of 16 November 2015, para 46, acknowledged that "*CNE activity could theoretically change the material on a computer*", but responded that it would be neither necessary, proportionate nor operationally sensible for an organisation such as GCHQ to make "*more than minimal, and to the greatest extent possible, transient, changes to targeted devices*":

105 Ciaran Martin, in his third witness statement of 24 November 2015, responded that GCHQ "*provide detailed information*" and that "*Ministers engage very significantly in the detail of the authorisation process and scrutinise carefully the methods that are employed*".

106 *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and GCHQ* [2016] UKIPTrib 14_85-CH, para 89.

107 Statement of MI5 witness to the IPT in *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others IPT/15/110/CH*, paras 37-43.

108 2015 SIA Report, chapter 7.

> "Bulk personal datasets comprise personal data relating to a number of individuals, the majority of whom are unlikely to be of intelligence interest. The security and intelligence agencies hold the data electronically and analysts will only look at the data relating to the minority who are of intelligence interest. The security and intelligence agencies do this by asking specific questions of the data to retrieve information of intelligence value."

2.71. Examples of specific BPDs given in the Operational Case include the passport register, the electoral register, the telephone directory and data about individuals with access to firearms. The categories disclosed to the IPT were:

(a) Law enforcement/intelligence: datasets containing operationally focused information from law enforcement or other intelligence agencies;

(b) Travel: datasets containing information which enables the identification of individuals' travel activity;

(c) Communications: datasets allowing the identification of individuals where the basis of information held is primarily related to communications data, e.g. a telephone directory;

(d) Finance: datasets allowing the identification of finance-related activity of individuals;

(e) Population: datasets providing population data or other information which could be used to help identify individuals, e.g. passport details; and

(f) Commercial: datasets providing details of corporations / individuals involved in commercial activities.

BPDs generally contain basic biographical details on individuals that will correspond to the definition of "*identifying data*". Dominic Grieve QC MP, Chair of the ISC which like the Review team saw the complete list of datasets, described some of them as "*pretty mundane*".[109] A small proportion contain material that is comparable to the content of communications as defined in the Bill.

2.72. The draft Code of Practice states:

> "The [Bill] does not create any new power to obtain BPDs. Rather it requires that the retention and use of BPDs must be subject to an authorisation scheme and a comprehensive set of robust and transparent safeguards. Specifically, [clause 183 of the Bill] provides that a [SIA] may not exercise a

[109] Hansard HC, 7 June, vol 611 col 1064.

power for the purpose of retaining or examining a BPD unless this is authorised by the issue of a warrant under Part 7 of the [Bill]."[110]

The power to acquire BPDs continues to exist, where acquisition is necessary and proportionate to the SIAs' statutory functions, under SSA 1989 and ISA 1994 (known as the information gateway provisions).

2.73. Personal data is defined for the purposes of Part 7 as data relating to an individual who can be identified from those data, or from those data and other information which is in the possession or, or likely to come into the possession of, the data controller (in this case, the relevant SIA).[111]

2.74. This power to retain and use BPDs differs from the other powers under review: for though (like them) the power in the Bill is exercisable only by the SIAs, the reality is that the NCA, police forces and other bodies also obtain, retain and use BPDs outside the scope of the Bill, and will continue to do so. Indeed it is well known that the analysis of bulk data is already conducted at a high degree of sophistication both within Government and, especially, in the private sector.[112]

How BPDs are obtained and used

2.75. BPDs are acquired both through overt and through covert channels. As recorded in the Operational Case (10.3), they are used on a daily basis, in combination with other capabilities, across the range of the SIAs' operations.

2.76. Two types of warrant are provided for in the Bill: class BPD warrants (which authorise the retention and use of a particular class of BPD) and specific BPD warrants. Because even a single BPD is likely to contain data on persons not currently targets, even the grant of a specific BPD warrant for the retention and use of a single BPD is considered for the purposes of this Review to be a bulk power.

2.77. A draft Code of Practice on the SIAs' retention and use of BPDs, very much fuller than the Code of February 2015, was published alongside the Bill on 1 March 2016. This sets out the detail of warrant applications, authorisation and approval of warrants, authorisation of the retention and use of BPDs falling within a warrant and safeguards.

---

110 Draft Code of Practice, *Security and intelligence agencies' retention and use of bulk personal datasets*, March 2016, 3.2.

111 Clause 182(2), building on the definition in the Data Protection Act 1988.

112 A flavour of this is given in AQOT 8.65-8.83 and the RUSI report 1.35-1.39 and 1.66-1.79: see further *Big Data: seizing opportunities, preserving values* (Executive Office of the [US] President, May 2014), and *The big data dilemma*, House of Commons Science and Technology Committee Fourth Report of Session 2015/16, HC 468, February 2016.

2.78. We received detailed briefings and demonstrations concerning the use of BPDs at both MI5 and MI6. We were introduced to the principal technical developments since 2005, inspected the complete list of BPDs that is currently in use, and questioned the SIAs about how those BPDs were obtained (in some cases, by means that would otherwise be unlawful, pursuant to ISA s7).

2.79. BPDs are still largely held by individual SIAs, though copies may be provided to other SIAs via the legal gateway provisions in SSA 1989 and ISA 1994, and individual officers may access data held by a different SIA on an ad hoc basis when authorised to do so. MI6 and MI5 currently have a greater reliance on BPDs than GCHQ. There is a cross-SIA mandate to work more collaboratively across the SIAs in sharing BPDs. The searching of BPDs is performed in a way that is analogous to commercial techniques.

2.80. The SIAs do not claim to employ searching techniques any more advanced than those available commercially: indeed I was told that they see themselves as "*catching up with the commercial sector*". The examples that we were shown appeared relatively straightforward, and were not indicative of the use of BPDs to predict in the highly sophisticated manner attributed to some private sector operatives. But any critical evaluation of the power needs to assume that SIAs have, or will acquire, the capability to make such use of BPDs as the most advanced current and future techniques allow.

Safeguards on BPDs

2.81. The internal SIA controls on the acquisition and use of BPDs, which include six-monthly reviews of each Agency's holdings, were summarised in the 2015 ISC Report[113] and the 2015 IsComm Report.[114] More detail will be given in the forthcoming annual report of the IsComm, to be published in September 2016.

2.82. The 2015 ISC Report criticised the absence of "*restrictions on the acquisition, storage, retention, sharing and destruction of [BPDs]*", and considered that oversight by the IsComm should be put on a statutory footing.

2.83. Those concerns have been largely met in the draft Bill and Code of Practice: the latest external safeguards on the use of BPDs are set out in the draft Code of Practice and summarised in the Operational Case (10.11-10.17). In summary:

(a) There is a new requirement to obtain warrants to retain and use BPDs, lasting six months and subject to the same "*double lock*" (Secretary of State and Judicial Commissioner) as warrants for bulk interception and bulk EI (clauses 183-186).

[113] 2015 ISC Report, paras 161-163.
[114] Report of the IsComm for 2014, June 2015, pp. 35-38.

(b) The Secretary of State (and the Judicial Commissioner on review) must be assured that the warrant is necessary in the interests of national security, or for the purposes of preventing or detecting serious crime, or in the interests of the economic well-being of the UK, so far as relevant to the interests of national security (clauses 185(3)(a), 186(5)(a)).

(c) They must similarly be assured that examination of the BPD is or may be necessary for the specified Operational Purposes, that examination of the BPD for each purpose is necessary on any of the grounds in (b) above and that the conduct authorised by the warrant is proportionate (clauses 186(5)(b)(c)).

(d) If a dataset is assessed to contain a significant component of intrusive data, applying the draft Code of Practice, it will have to be authorised by a specific BPD warrant rather than a class BPD warrant.

(e) Provisions for the handling, retention, destruction and audit are set out in the draft Code of Practice (section 7), and will be subject to audit by the IPC, including its technical inspectorate (draft Code of Practice, section 9).

(f) Additional safeguards apply for health records (clause 187) and sensitive professions (draft Code of Practice, 7.8-7.10).

2.84. It has come to my attention that some BPDs may contain material that is comparable to the content of communications, and in rare cases even material subject to LPP. In the light of these facts I have already recommended to the Home Office that consideration be given to the introduction of additional safeguards to the Bill and Code of Practice.

2.85. The acquisition, retention and use of BPDs is subject to the oversight of the IsComm, and will be overseen by the IPC in future.

Criticism of BPDs

2.86. In the ongoing IPT case on BPDs and s94, Privacy International drew attention in its Statement of Grounds to what was described as:

(a) the large size of some BPDs (e.g. the fact that there are 19 million Nectar cardholders, the details of whom might be held in a BPD);

(b) the ability of analysts to link BPDs together so as to find all relevant information from one search query;

(c) "*minimal oversight*" and "*no clear legal regime*" in the past;

(d) the powers of the SIAs to obtain BPDs by means of theft, bribery and coercion; and

(e) abuse of BPDs by staff at the SIAs, which reported to the ISC that "*they had disciplined – or in some cases dismissed – staff for inappropriately accessing personal information held in these datasets in recent years*".[115]

2.87. Further concerns were set out in written evidence by Eric King to the Joint Bill Committee in December 2015.[116] These included intelligence sharing, the personal nature of some travel, financial and health-related databases, and the absence of any published review.

[115] 2015 ISC Report, para 163(i). Cf. Andrew Griffin, "British spies hacked themselves and family members to get personal information to send birthday cards, new papers reveal", The Independent, 21 April 2016, referred to by Joanna Cherry QC MP in the Report stage debate on the Bill, 7 June 2016.

[116] IPB0106, evidence submitted by Eric King to the Joint Bill Committee on 21 December 2015: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/draft-investigatory-powers-bill-committee/draft-investigatory-powers-bill/written/26357.html.

3. PREVIOUS ASSESSMENTS

Introduction

3.1. Despite three preparatory studies, pre-legislative and legislative scrutiny by multiple parliamentary committees and the Government's presentation in March 2016 of the Operational Case, consideration of the Bill has to date featured no authoritative independent analysis of the operational case for the powers under review.

3.2. But it is important to note that with the exception of bulk EI (1.19 above), each of the powers under review:

(a) has already been in use for at least several years; and

(b) has been the subject of comment as to its utility and/or necessity by one or more of the dedicated oversight and scrutiny bodies for which the law provides.

The utility of the bulk interception power was also addressed in AQOT, as summarised at 1.25-1.27 above.

3.3. In addition to the dedicated oversight and scrutiny bodies, others have also commented on the utility of the powers under review, or analogous powers.

3.4. This chapter first identifies the bodies and individuals that have already addressed the operational case for the powers under review, and then summarises their conclusions.

Dedicated oversight and scrutiny bodies

3.5. All four of the powers under review are subject to external oversight and scrutiny by:

(a) ***the two Commissioners*** appointed for the purpose, former Lord Justices of Appeal whose functions will be subsumed into those of the IPC:[117]

- the IOCC , currently Rt. Hon. Sir Stanley Burnton, who with his office IOCCO is responsible for oversight of oversight of bulk interception, and (from March 2015) of bulk acquisition;[118] and

[117] Bill, clauses 203-215. Lord and Lady Justices of Appeal are the most senior tier of judges in England and Wales, save only for Justices of the Supreme Court.

[118] See further AQOT 6.100-6.104. IOCCO has had oversight of MI5's access to bulk communications data acquired pursuant to the s94 power since 2007: that access followed the authorisation process set out in RIPA 2000 s 22 and 23.

- the IsComm, currently Rt. Hon. Sir Mark Waller, who is responsible with his staff for the oversight of EI and of BPDs;[119]

(a) ***the ISC***, which is the parliamentary body tasked with providing oversight of the use of investigatory powers by the SIAs;[120] and

(b) ***the IPT***, the independent tribunal which will have jurisdiction to determine complaints about the alleged exercise of each of the powers under review (as it has in relation to their current equivalents).[121]

All those bodies have the necessary security clearance to investigate thoroughly the activities with whose oversight or scrutiny they are charged.

Other bodies and individuals

3.6. Comments on the utility of the powers under review, or similar powers, have also been made by:

(a) the PCLOB (USA);

(b) the NAS (USA);

(c) former intelligence officials, in evidence to Parliament and elsewhere;

(d) the ECtHR;

(e) the CJEU; and

(f) the SURVEILLE project of the European Union.

Of those, the first three had access to classified materials and the last three did not.

3.7. The assessments of the above bodies and individuals are summarised in the remainder of this chapter.

(1) Assessments of the Interception of Communications Commissioner

3.8. As noted above, IOCCO has oversight of ***bulk interception***, and (since 2006 in respect of MI5 and February 2015 in respect of GCHQ) ***bulk acquisition***.

---

119 Some BPDs are obtained by interception, which is overseen by IOCCO: but as BPDs they are subject to the oversight of the IsComm. Before February 2015, the IsComm also had oversight of bulk acquisition under TA 1984 s94.

120 See AQOT 6.112-6.113.

121 See AQOT 6.105-6.111. A right of appeal from certain judgments of the IPT is introduced by the Bill (clause 217).

3.9. In relation to ***bulk interception***, the IOCC's statutory role is to audit compliance against existing legislation and to investigate any contraventions of the legislation (whether detected during IOCCO inspections or self-reported by the SIAs). When reviewing interception warrants, including warrants for interception in bulk, IOCCO scrutinises the SIAs' justifications for necessity and proportionality on a case-by-case basis, both in the interception warrant application itself and then at the second stage of the process where the analysts submit justifications to select and examine material from the bulk. It interviews operational staff about those justifications, about how the material acquired has been used and whether it achieved the objectives set out in the application. Cancellation of warrants may be recommended if they are excessively intrusive or if they do not produce sufficient information to be proportionate. IOCCO also examine the safeguards in place to protect privacy and the arrangements for the retention, storage and destruction of any material obtained.[122]

3.10. The IOCC has also expressed more general views on the utility, necessity and intrusiveness of bulk interception.[123] In April 2014, no doubt prompted by the Snowden allegations, the IOCC raised and answered a number of "*Questions of Concern*" relating to the current bulk interception power in RIPA 2000 s8(4):

(a) On the question of whether "*it is in general necessary and proportionate to warrant the initial interception of this kind and volume of material*", the IOCC indicated that it would be, subject to satisfactory safeguards including proper arrangements for its treatment, lawful examination and retention.[124]

(b) On the question of whether "*there are other reasonable less intrusive means of obtaining the information which it is considered necessary to obtain*", the IOCC stated:

> "I am satisfied that at present there are no other reasonable means that would enable the interception agencies to have access to external communications which the Secretary of State judges it is necessary for them to obtain for a statutory purpose under the section 8(4) procedure. This is a sensitive matter of considerable technical complexity which I have investigated in detail."[125]

---

122 See, e.g., IOCCO's March 2015 report at 6.46-6.49 (inspection regime), 6.60-6.65 (retention, storage & destruction), 6.66-6.81 (inspection findings) and 6.82-6.97 (contraventions / errors).

123 Supplementing strong views previously expressed by both Commissioners as to the utility of interception in general (not limited to bulk): 2011 Annual Report of the IsComm, p. 23 ("*Operational successes*"); 2011 Annual Report of the IOCC, chapter 5 ("*Successes*"); 2012 Annual Report of the IOCC, July 2013, Foreword.

124 2013 Annual Report of the IOCC, April 2014, 5.5.50.

125 *Ibid.*, 6.5.51.

3.11. The IOCC also gave detailed reasons for concluding that the s8(4) process for bulk interception "*does not have a significant risk of undue invasion of privacy*".[126] He described as "*a matter of policy*" the question of whether the SIAs should continue to be enabled to intercept external communications in order to assist their functions of protecting the nation and its citizens, but expressed the personal view that it was "*obvious*" that they should.

3.12. As to ***bulk acquisition***, IOCCO published a report in July 2016 setting out the findings of its first review of the use of section 94 directions to acquire bulk communications data. The purpose of IOCCO's review was to identify the extent to which the SIAs use section 94 directions, to assess what a comprehensive oversight and audit function of section 94 directions would look like and to assess whether the systems and procedures in place for section 94 directions are sufficient to comply with the legislation and any relevant policies. As such the review report does not focus specifically on utility, although it does contains one indication of it. The section entitled "*The operational case for bulk communications data being acquired and retained by the agencies*" (8.27-8.32) notes the existence of this Review and comments (at 8.29) that:

> "It is clear from our oversight that access to bulk communications data retained by the agencies pursuant to section 94 directions enables more complex analysis to be undertaken which would not be possible through a series of individual requests [to CSPs] made under Chapter 2 of Part 1 of RIPA."

3.13. To summarise, implicit in IOCCO's function is the examination of the utility to be obtained from bulk interception and acquisition.[127] Whilst it has never had to address itself explicitly to the subject-matter of this Review:

(a) It may be inferred from IOCCO's reviews of the lawfulness of bulk interception (including its necessity) that successive IOCCs have considered that power to be a useful one.

(b) The IOCC expressed satisfaction in his report of April 2014, after detailed technical examination, that there were no reasonable alternatives to bulk interception.

(c) The utility of the bulk acquisition power for the purposes of complex analysis not possible under other powers was noted in the IOCC's report of July 2016.

---

126 *Ibid.*,. 6.5.43. See also 6.6.2: "*The interception agencies do not engage in indiscriminate random mass intrusion by misusing their powers under RIPA 2000 Part I. It would be comprehensively unlawful if they did.*"

127 The Bill extends the statutory oversight function of the existing Commissioners by including an explicit provision for the IPC to report on the results of the use of the powers, including their impact: clause 210(2)(b).

(2) Assessments of the Intelligence Services Commissioner

3.14. As noted in chapter 2 above, the IsComm has oversight of ***bulk EI*** and of ***BPDs***. Before February 2015, the IsComm also had oversight of GCHQ's ***bulk acquisition*** under TA 1984 s94

3.15. The current IsComm has overseen the SIAs' use of EI since 2011, but until now his reports on it have been confined to confidential annexes. The first open report on EI is likely to be published in September 2016. There has been no assessment of the proposed ***bulk EI*** power, if only because the existing law makes no express provision for it.[128]

3.16. As to ***BPDs***, between 2011 and 2014, the IsComm reported on the use of BPDs in secret annexes (which I have read). Even the fact that the IsComm was reporting on their use was not publicly known. But reports were produced (and continue to be produced) in which conscientious consideration was given to the acquisition, use and retention of BPDs.

3.17. The conclusions of Sir Peter Gibson (in 2011) and of Sir Mark Waller (in 2012-2014) were variously supportive of (or, where no view was expressed, consistent with) the utility of BPD regime and its operation in accordance with the requirements of necessity and proportionality.

3.18. In 2015, Sir Mark Waller reported publicly on the use of BPDs for the first time. He disclosed the existence of internal review bodies which consider the retention of datasets, and stated that it was his practice to "*assess whether the review bodies have properly applied the test of necessity and proportionality in retaining and making the data available*" and to "*inspect how members of the intelligence services access the data sets .. as well as reviewing how they apply the necessity and proportionality justifications of intrusion into private information*".[129]

3.19. The IsComm asked for explanations of how the datasets selected for close examination were used, and stated:

> "In essence the justification will be that although the particular dataset has information on individuals of no intelligence interest it will also have important information on persons who will be or are of intelligence interest and will

---

[128] The IsComm has expressed concerns about the over-broad use of "*thematic*" property warrants under ISA 1994 s5: Report of the IsComm for 2014, June 2015, pp. 18-19. But those concerns appear to stem from the narrow terms of s5 rather than from the undesirability in principle of a warrant that does not identify each of the individuals subject to it. This may be seen from the fact that no equivalent concerns are expressed in relation to warrants under ISA 1994 s7, which makes specific reference to thematic or "*class*" authorisation: pp. 18, 24-26.

[129] Report of the Intelligence Services Commissioner for 2014, June 2015, pp. 34-35.

provide important links assisting in the identification or movements of those individuals".[130]

The IsComm concluded that "*[t]he case for holding BPD has been established in each service*" and made a number of recommendations, mostly aimed at improving privacy protections.[131]

3.20. Further detailed reporting on the use of BPDs is expected in the IsComm's next report, which will be published in September 2016.

3.21. As to ***bulk acquisition***, nothing was published openly in the period 2011-2014, since the capability had not been avowed, but I have inspected the relevant confidential annexes in relation to GCHQ. The report for 2013 endorsed the necessity and proportionality of the capability as used by GCHQ, by reference to the number of intelligence reports that were based on the data acquired. The first public review of bulk acquisition was published by the IOCC in July 2016 (3.12 above).

(3) Assessments of the Intelligence and Security Committee of Parliament

3.22. The ISC considered the utility of some or all of the powers under review in its reports of March 2015 and February 2016.[132] Comments of ISC members during the passage of the Bill, in particular at second reading and report stage in the House of Commons and at second reading in the House of Lords, reflect further evidence taken by the ISC after the 2016 ISC report.

3.23. I summarise below the views expressed by the ISC and its members on the operational case for the powers under review. I do not summarise (because they are not relevant to the subject-matter of this report) the ISC's detailed evaluation of the applicable safeguards (internal and external), or its many recommendations in both 2015 and 2016, some of which influenced the shape and content of the Bill and others of which have been advanced in the form of proposed amendments to it.

2015 ISC Report

3.24. The 2015 ISC Report concluded, after what was described as "*a detailed* investigation *into the intrusive capabilities that are used by the UK intelligence and security Agencies*",[133] that "*the investigatory powers the Agencies were authorised to employ* were *necessary and proportionate*".[134] Some of its reasons

130 *Ibid.*, p.35.
131 *Ibid.*, p.38.
132 See fnn 16 and 29 above.
133 2015 ISC Report, Key Findings (v) (p.1).
134 As summarised in the 2016 ISC Report, Introduction, para 2.

for that conclusion were redacted from the open version of the report, but I have read all the evidence that was placed before the ISC, a good deal of which concerned the utility of the bulk powers, as well as the full version of the report.

Bulk interception

3.25. The utility of ***bulk interception*** was considered at paras 78-90 of the 2015 ISC Report, which were written after the ISC had:

> "questioned GCHQ in detail as to how useful bulk interception really is, and sought evidence as to how the capability has been used and why the intelligence gained could not have been gathered using any other capability".

3.26. The ISC ***concluded*** that:

> "We were surprised to discover that ***the primary value to GCHQ of bulk interception was not in reading the actual content of communications, but in the information associated with those communications***. This included both Communications Data (CD) as described in RIPA (which is limited to the basic 'who, when and where' ...), and other information derived from the content (which we refer to as Content-Derived Information, or CDI), including the characteristics of the communication.
> ...
>
> The examples GCHQ have provided, together with the other evidence we have taken, have satisfied the Committee that ***GCHQ's bulk interception capability is used primarily to find patterns in, or characteristics of, online communications which indicate involvement in threats to national security***. The people involved in these communications are sometimes already known, in which case valuable extra intelligence may be obtained (e.g. a new person in a terrorist network, a new location to be monitored, or a new selector to be targeted). In other cases, it exposes previously unknown individuals or plots that threaten our security which would not otherwise be detected.
> ...
>
> We are satisfied that current legislative arrangements and practice are designed to prevent innocent people's communications being read. Based on that understanding, we acknowledge that ***GCHQ's bulk interception is a valuable capability that should remain available to them***."

(emphasis added).

Bulk acquisition

3.27. Confirming a view expressed in its 2013 report on the Communications Data Bill, the ISC referred to access to communications data as "*a critical capability*".[135]

3.28. Because the bulk acquisition capability under TA 1984 s94 was not avowed until November 2015, the parts of the ISC's report that referred specifically to the use of that capability were omitted from the open version.[136] No opinion was expressed, in the open or closed version, as to the utility of the bulk acquisition power.

Bulk EI

3.29. The ISC referred to CNE in a short and heavily-redacted part of its 2015 Report.[137] While no detailed account of its utility was given, an acceptance of its utility might be cautiously inferred from the open comments that "*Agencies may undertake IT Operations against computers or networks in order to obtain intelligence*" and that this work was growing.

3.30. Even in the closed version of the ISC's report, no specific mention was made of bulk EI (in keeping with the February 2015 Code of Practice, which avowed EI for the first time but also said nothing specific about bulk EI). This is unsurprising in view of the fact that bulk EI had not (and has not) been used.

Bulk personal datasets

3.31. The ISC examined the SIAs' use of BPDs in chapter 7 of its March 2015 report, citing the views of MI6 that BPDs:

> "... 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",

and of GCHQ that:

> "they consider Bulk Personal Datasets to be an increasingly important investigative tool, which they use primarily to 'enrich' information that has been obtained through other techniques".[138]

---

135 2015 ISC report, U (after para 132).
136 In particular, paras 134(ii), 147-150.
137 2015 ISC Report, Box and CC (p. 67).
138 2015 ISC Report, paras 152-153. Further citation of evidence (which I have read) was redacted from the open Report.

3.32. The ISC appears to have agreed, concluding in relation to utility that:

> "The Agencies use Bulk Personal Datasets – large databases containing personal information about a wide range of people – to identify individuals in the course of investigations, to establish links, and as a means of verifying information obtained through other sources. These datasets are an increasingly important investigative tool for the Agencies."[139]

2016 ISC report

3.33. In its report of February 2016, the ISC stated that it remained of the view (expressed by a differently-constituted ISC in March 2015) that "*the investigatory powers the Agencies were authorised to employ were necessary and proportionate*" (Introduction, para 2). It acknowledged, in particular, that "*the Agencies need the capability to conduct Equipment Interference as necessary*", but stated that:

> "the Committee has not been provided with sufficiently compelling evidence as to why the Agencies required Bulk Equipment Interference warrants, given how broadly Targeted Equipment Interference Warrants can be drawn".

3.34. Similarly, in relation to BPDs, the ISC did not doubt their utility but questioned the need for class warrants which would enable multiple BPDs to be obtained without specific Ministerial consideration of the degree of intrusion into privacy effected by each one.

3.35. Each of those conclusions was however subsequently qualified by the Chair of the ISC, after consideration of further extensive classified evidence provided to the ISC, as indicated below.

Comments of ISC Chair

3.36. In relation to ***bulk EI***, the Chair of the ISC (elected by the ISC members), the former Attorney General Dominic Grieve QC MP, stated at report stage that having carefully scrutinised the additional evidence provided since the 2016 ISC report:

> "... we concluded that there were circumstances – target discovery was an example – that would require a bulk equipment interference warrant and could not simply be covered by a thematic warrant*".*[140]

That concession was subject to a request for further assurances and safeguards, which were provided.

---

139 U, after para 163.

140 Hansard HC, 6 June 2016, vol 611 col 895.

3.37. On the following day, Mr Grieve told the House of Commons that subject to safeguards to ensure their use was limited (again, subsequently provided), he was satisfied that class warrants were appropriate when the privacy considerations were identical.[141]

3.38. More generally, he reiterated the operational case for bulk powers as follows:

> "[i]f there were not bulk powers to enable the Agencies to look to intercept bulk and then to search it to find what they are looking for, it would be very difficult for the Agencies to defend our security both against espionage and particularly terrorism. That is the reality."[142]

(4) Proceedings in the IPT

3.39. The IPT regards itself as having "*very distinct advantages over both the Commissioner and the ISC*", prominent among them its ability not only to access all secret material but to hold *inter partes* hearings at which "*forceful legal submissions can be made on behalf of Claimants who seek to criticise the system*".[143]

3.40. That said, the IPT has not so far been called upon to answer the question at the heart of this Review: how strong is the operational case for the bulk powers, and could equivalent results be achieved by other means?

3.41. The IPT has looked at ***bulk interception*** in two cases, dating from 2004 and 2014-2015.[144] It looked at ***bulk EI*** in a judgment of February 2016,[145] and is considering ***bulk acquisition*** and ***BPDs*** in a pending case.[146]

3.42. No material disagreement was expressed in those cases with SIA witnesses whose evidence stated or assumed the utility of the powers with which the cases were concerned. It is fair to say though that in none of the cases was the IPT required to adjudicate on a submission that the bulk powers were useless, or to evaluate the operational case for them. As the IPT recently stated: "*It is not .. our role, as it is that of the Commissioners, to supervise and oversee the performance of the Agencies. Our role is to investigate individual complaints that*

---

141 Hansard HC, 7 June 2016, vol 611 col 1063.

142 Hansard HC 7 June 2016, vol 611 col 1059.

143 *Liberty v Secretary of State for the Foreign and Commonwealth Office and others* [2014] UKIPTrib 13_77-H, para 46.

144 *British-Irish Rights Watch v Security Service, SIS and GCHQ* IPT/01/77 (2004); *Liberty and others v Security Service, SIS, GCHQ* IPT/13/77/H.

145 *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and GCHQ* [2016] UKIPTrib 14_85-CH.

146 *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and others* IPT/15/110/CH.

are made to us, after establishing the legal framework which is to apply to them".[147]

(5) Assessments by the Privacy and Civil Liberties Board (USA)

3.43. The Privacy and Civil Liberties Board **[PCLOB]** is an independent bipartisan agency within the US executive branch, established by the Implementing Recommendations of the 9/11 Commission Act of 2007 but beginning operations as an independent agency only in August 2012. Its oversight mandate is limited to those measures taken by the government to protect the nation from terrorism.[148] The Board comprises four part-time members and a full-time chairman, all of them distinguished academic and/or practising lawyers who were appointed by the President and confirmed by the Senate. Both they and their small staff hold very high levels of security clearance.

3.44. The PCLOB has produced two reports to date on programmes associated with bulk collection. Significant parts of those reports consist of statutory and constitutional analysis, which are US-specific and concern matters which are outside the remit of this Review. The PCLOB's analysis of the privacy and civil liberties implications of the programmes that it reviewed, and its recommendations regarding safeguards, are also beyond the scope of this Review.

3.45. But both reports also expressed firm and reasoned conclusions on the utility of the programmes that they reviewed. The first of them in particular has been heavily relied upon by NGOs and others seeking to challenge the utility of bulk powers in the UK.

3.46. The two reports, and the extent of their relevance in the UK context, are summarised below.

Section 215 telephone records programme

3.47. The PCLOB's first report was on the telephone records programme conducted under an order that was issued by the Foreign Intelligence Surveillance Court **[FISC]** under s215 of the USA PATRIOT Act and renewed approximately every 90 days.[149] In the PCLOB's summary:

> "The FISC order authorizes the NSA to collect nearly all call detail records generated by certain telephone companies in the United States, and specifies

147 *Human Rights Watch Inc. and others v Secretary of State for the Foreign and Commonwealth Office*, [2016] UKIPTrib15 165-CH, 16 May 2016, para 44.

148 42 USC §2000ee.

149 PCLOB, *Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the FISC*, January 2014.

detailed rules for the use and retention of these records. Call detail records typically include much of the information that appears on a customer's telephone bill: the date and time of a call, its duration, and the participating telephone numbers. ... The records collected by the NSA under this program do not, however, include the content of any telephone conversation. After collecting these telephone records, the NSA stores them in a centralized database."

3.48. Following the PCLOB report, the s215 programme was allowed to lapse but was replaced by a new programme under the USA Freedom Act. The bulk collection of telephone metadata *by the NSA* has therefore ceased. But under the new programme, "*telephone metadata*" collected *by service providers* is still made accessible to the NSA. The bulk collection of such data thus continues on the basis of the broad definition of bulk (1.5-1.6 above), though not on the narrow definition favoured in the USA and in the Bill (1.7-1.8 above): see further 3.65 below.

3.49. It should also be noted that Jim Comey, Director of the FBI, was quoted in late 2015 as saying that the replacement programme in the USA Freedom Act "*should work as well or better than what we used to have*".[150]

Comparison with UK bulk powers

3.50. On the basis of the summary description quoted above, the s215 programme has obvious similarities with the bulk acquisition power described at 2.29-2.45 above. In particular:

(a) Each programme allows for the storage of telephone communications data (or metadata, in the US terminology) in a single database.

(b) The "*call detail records*" described by the PCLOB fall within the definition of the "*traffic data*" to which all current s94 directions for bulk communications data apply.

3.51. My potential to comment further is limited by the degree of public disclosure in relation to these programmes that has been deemed possible, both in the US and in the UK. But it would be wrong to assume that the two programmes are identical, or even close equivalents. In particular:

(a) ***Nature of communications:*** The s215 power is limited to the collection of "*telephone records*" relating to "*calls*". The UK bulk acquisition power relates to "*communications data*", a category which is capable of including data

[150] https://morningconsult.com/2015/12/09/comey-effectiveness-of-usa-freedom-act-not-yet-clear/.

relating also (for example) to emails, texts and VOIP (voice over internet protocol) telephony.[151]

(b) ***Types of provider:*** The PCLOB report states that those telephone records are obtained from "*certain telephone companies in the United States*" (p. 8), apparently including landline providers (p. 23). But the report does not specify (any more than does IOCCO in the UK) whether records were obtained from mobile providers, and if so to what extent. US "*current and former officials*" were quoted in February 2014 as saying that the NSA was only collecting "*between 20 and 30 percent*" of US call data, the shortfall reflecting "*Americans' increasing shift from landline to cellphone use*".[152] The President's Review Group on Intelligence and Communications Technologies similarly recorded that "*the meta-data captured by the program covers only a portion of the records of only a few telephone service providers*".[153]

(c) ***Categories of records:*** The records collected under the s215 power, again according to PCLOB, typically included "*the date and time of a call, its duration, and the participating telephone numbers*". They did not include cell site location information.[154] The UK category of "*traffic data*", to which each of the current s94 directions relates, is potentially broader: in particular, it extends to location data and other related material.[155] Under the Bill, the power will continue to extend to "*any communications data*", with no statutory exclusion even for ICRs.[156]

(d) ***Permitted uses:*** The only purpose for which "*NSA analysts were permitted to search the s215 calling records housed in the agency's database*" was "*to conduct queries .. designed to build contact chains leading outward from a target to other telephone numbers*", on the basis of "*a reasonable, articulable suspicion (RAS) that the number is associated with terrorism*".[157] But as demonstrated by IOCCO's reference to "*complex analysis*" (8.29), and by the fact that no RAS is required under current UK law or under the Bill, UK analysts have a considerably wider range of uses for their records.

(e) ***Scale of use:*** The scale of use of the two programmes is very different. In 2012, the NSA (which is a foreign-focused organisation) queried only "*around*

---

151 See draft Bulk Acquisition code of practice, March 2016, 2.13.

152 Ellen Nakshima, "NSA is collecting less than 30% of US call data, officials say", Washington Post, 7 February 2014.

153 "NSA Report: liberty and security in a changing world", December 2013, chapter 3, p.57.

154 PCLOB section 215 report, p. 22.

155 IOCCO July 2016 report, 8.3 and 8.34.

156 Though internet connection records are not currently acquired under the bulk acquisition power in s94: fn 85 above.

157 PCLOB section 215 report, pp. 27, 9. Contact-chaining enables analysts to retrieve the numbers directly in contact with the seed number ("*the first hop*") and also numbers in contact with those numbers ("*the second hop*"). A third hop was formerly allowed as well.

300 seed numbers".[158] In 2015, by contrast, MI5 made 20,042 applications to access communications data obtained pursuant to s94 directions, relating to 122,579 items of communications data, and GCHQ identified 141,251 communications addresses or identifiers of interest from such communications data, which directly contributed to an intelligence report.[159] That is despite the fact that data under s215 was retained for five years, as against 12 months under the UK power.

Utility of the s215 programme

3.52. The PCLOB found that, as a matter of US law, the telephone records program did not have an adequate basis in s215 and that it also raised constitutional concerns. But of greater relevance to this Review is the PCLOB's finding that the program had "*shown minimal value in safeguarding the nation from terrorism*". It summarised its conclusions as follows:

> "Based on the information provided to the Board, including classified briefings and documentation, we have not identified a single instance involving a threat to the United States in which the program made a concrete difference in the outcome of a counterterrorism investigation. Moreover we are aware of no instance in which the program directly contributed to the discovery of a previously unknown terrorist plot or the disruption of a terrorist attack. And we believe that in only one instance over the past seven years has the program arguably contributed to the identification of an unknown terrorist suspect. Even in that case, the suspect was not involved in planning a terrorist attack and there is no reason to believe that the FBI may have discovered him without the contribution of the NSA's program.
>
> The Board's review suggests that where the telephone records collected by the NSA under its s215 program have provided value, they have done so primarily in two ways: by offering additional leads regarding the contacts of terrorism suspects already known to investigators, and by demonstrating that foreign terrorist plots do *not* have a US nexus. The former can help investigators confirm suspicions about the target of an inquiry or about persons in contact with that target. The latter can help the intelligence community focus its limited investigatory resources by avoiding false leads and channelling efforts where they are needed most. But with respect to the former, our review suggests that the Section 215 program offers little unique value but largely duplicates the FBI's own information gathering efforts. And with respect to the latter, while the value of proper resource allocation in time-sensitive situations is not to be discounted, we question whether the American public should accept the government's routine collection of all of its

158 PCLOB section 215 report, p.30.
159 IOCCO July 2016 report, 8.62 and 8.70.

telephone records because it helps in cases where there is no threat to the United States."[160]

Conclusion

3.53. The PCLOB's conclusion that s215 had minimal value in protecting the USA from terrorism echoed comments made by the President's Review Board on Intelligence and Communications Technologies, was not doubted by the NAS Report (p. 57) and is of course not questioned by me.

3.54. But that conclusion cannot simply be read over to the bulk acquisition power in the Bill, because of the significant and material differences between the two powers. In particular:

(a) The nature of the communications subject to the two powers, the types of provider from whom it is collected and the categories of records collected cannot be assumed to be the same (3.51(a)(b)(c) above).

(b) The purposes for which the UK data may be used are considerably broader than those available to the NSA, and the frequency of use is on a completely different scale (3.51(d) above and 6.9-6.11 below).

(c) The 25 case studies in Annex 9, on which we have commented at 6.12-6.36 below, together with the internal documents summarised at 6.39-6.43 below, demonstrate the utility of bulk acquisition power, particularly in relation to the domestic terrorist threat (including live attack plans), but also in relation to travel to Syria, counter-proliferation and counter-espionage.

Section 702 surveillance programme

3.55. The PCLOB came to a much more positive conclusion about the utility of FISA s702, a power under which the US Government with the compelled assistance of CSPs "*collects the contents of electronic communications, including telephone calls and emails, where the target is reasonably believed to be a non-US person located outside the United States*".[161]

---

160 s215 report, pp. 11-12. Similar conclusions were expressed by the President's Review Group on Intelligence and Communications Technologies in its "NSA Report: liberty and security in a changing world", December 2013, chapter 3 p.57: "*[T]he information contributed to terrorist investigations by the use of section 215 telephony meta-data was not essential to preventing attacks and could readily have been obtained in a timely manner using conventional section 215 orders*".

161 PCLOB, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, July 2014, p.1. In contrast to its predecessor the s702 report received a critical reaction from privacy advocates: "NSA reformers dismayed after privacy board vindicates surveillance dragnet", The Guardian, 2 July 2014.

Similarities with UK bulk powers

3.56. There are marked similarities between the s702 programme and bulk interception as practised in the UK, particularly via the "*strong selector process*" summarised at 2.19(a) above:[162]

(a) Both are foreign-focused capabilities, based on the interception of a cable and the collection of "*wanted*" communications by the application of strong selectors.

(b) The application of those selectors from a very early stage gives both the flavour of targeted capabilities, though as explained at 2.19(a) above, the holding of communications in bulk for a short period means that a bulk warrant will be required under the Bill.[163]

(c) Both offer the advantages of operational scale and flexibility to service the range of foreign intelligence missions.

(d) Even the authorisation regimes are similar, with external authorisation of the intelligence purposes for which the data can be accessed and used and the procedures for targeting and handling of information, but with decisions relating to individual selectors being delegated to GCHQ / NSA.[164]

Utility of the s702 programme

3.57. The PCLOB devoted seven pages of its report to the value of the s702 programme. Its analysis was limited to "*the counterterrorism value*" of the programme, though it noted that *"the programme serves a broader range of foreign intelligence purposes*".

---

[162] As there noted, the ISC preferred to think of this process as targeted rather than bulk collection: the PCLOB, similarly, characterised s702 as "*acquiring the communications of specifically targeted foreign persons who are located outside the United States*": p.9. It would appear nonetheless from p.56 of the PCLOB s702 report that the scale of data generated by s702 is sufficient to allow for "*at times complex queries across large datasets*" – a capability that is reminiscent of the "*complex query process*" described at 2.19(b) above.

[163] The PCLOB described s702 as authorising the targeting of persons (pp.20-21).

[164] PCLOB s702 report, p.106: "*Targeting decisions are made by NSA analysts and reviewed only within the executive branch.*" There are of course differences in the applicable safeguards: for example, s702 selectors may not be applied to US citizens (whereas UK citizenship is a relevant consideration neither under RIPA nor under the Bill); on the other hand, UK warrants last six months rather than a year; and the UK has much shorter retention periods for data collected under bulk warrants than the five years referred to at p. 60 of the PCLOB s702 report.

3.58. In summary, the PCLOB concluded that the s702 programme:

(a) "*makes a substantial contribution to the government's efforts to learn about the membership, goals and activities of international terrorist organizations, and to prevent acts of terrorism from coming to fruition*; and

(b) "*allows the government to acquire a greater range of foreign intelligence than it otherwise would be able to obtain, and .. provides a degree of flexibility not offered by comparable surveillance authorities*".

That flexibility stemmed, in part, from the considerable freedom granted to the NSA to target non-US persons located abroad, permitting the targeting of people who "*are not themselves involved in terrorism or any illegitimate activity*" and allowing the government "*to quickly begin monitoring new targets and communications facilities without the delay occasioned by the requirement to secure approval from the FISA court for each targeting decision*".

3.59. Specifically, information derived from the use of s702 has:

(a) "*helped the United States learn more about the membership, leadership structure, priorities, tactics, and plans of international terrorist organizations*";

(b) "*enabled the discovery of previously unknown terrorist plots directed against the United States and foreign countries, enabling the disruption of those plots*"; and

(c) "*been used to monitor individuals believed to be involved in terrorism*".

3.60. In the terminology of the UK SIAs, therefore (4.7 below), intelligence derived from the use of s702 is useful at all three stages of security and intelligence work: *identify*, *understand* and *action.* The PCLOB commented that:

> "Because surveillance is conducted on an individualized basis where there is reason to target a particular person, it is perhaps unsurprising that the program yields a good deal of information."

The same could equally be said of the process described at 2.19(a) above.

3.61. In terms of intelligence reporting, the PCLOB commented that:

> "over a quarter of the NSA's reports concerning international terrorism include information based in whole or in part on Section 702 collection, and this percentage has increased every year since the statute was enacted. These reports are used by the recipient agencies and departments for a variety of purposes, including to inform senior leaders in government and for operational planning."

The number of signals intelligence reports based on s702 was said to have "*increased exponentially*" since 2008.

3.62. The fact that strong selectors are already known when data is accessed under s702 raises the question of why a targeted warrant would not be an acceptable alternative. The PCLOB's answer was that the less rigorous procedures necessary for the use of s702 permitted "*greater flexibility and a dramatic increase in the number of people who can realistically be targeted*".[165] See further 5.22 below.

PCLOB - conclusion

3.63. The conclusions of the PCLOB in its s215 report have been heavily relied upon for the proposition that bulk powers such as those under review are useless or of limited utility.

3.64. But on close analysis, the reality turns out to be different:

(a) The bulk acquisition power in the Bill is different in its nature from the s215 power: there is no reason to assume that its utility is similarly limited (and there is much evidence that it is not: chapter 6 below).

(b) The bulk interception power in the Bill, as described at 2.19(a) above, is very similar to the s702 power which the PCLOB found to have a high and increasing value in fighting terrorism.

3.65. More broadly, it is not wholly accurate to suggest – as some have done – that the US has turned away from bulk, in the broader sense of that word (1.5 above) or even in the narrower sense (1.7 above). The USA Freedom Act did mark the end of a capability to acquire metadata in bulk – a capability found by two review bodies to have been of very limited utility. However:

(a) The s215 replacement capability, which the FBI anticipated would be at least as useful as the power it replaced (3.49 above), permits the targeted querying of communications retained by service providers. The large amounts of data from which the targeted selection is made continue to include a significant portion that is not associated with current intelligence targets.

(b) The s702 arrangements continue to permit the targeted selection and retention by the NSA of wanted communications from bulk internet traffic, in very much the same way as the strong selector process described at 2.19(a) above.

[165] PCLOB s702 report, p.106.

(c) The broadly-phrased Executive Order 12333, currently under review by the PCLOB, implicitly authorises an extremely wide range of techniques for use outside the USA, whereby data may be acquired in bulk as a basis for subsequent selection.

(d) As a US interlocutor pointed out to me, there are also "*bulk*" elements (as in the UK) to many other powers: for example anti-money laundering programmes which require banks to report all transactions above a certain level, and requirements on airlines to furnish passenger name records, most of which do not relate to current targets, to the US Government.

(6) National Academy of Sciences Report

3.66. In 2014, the White House issued Presidential Policy Directive 28 **[PPD-28]**, which requested the Director of National Intelligence to assess the feasibility of alternatives to bulk collection for the US intelligence community.[166]

3.67. The resultant NAS Report, published in 2015, was the culmination of a study conducted by a security-cleared committee whose nine members (supported by three consultants and four staff) included:

> "individuals with expertise in national security law; counterterrorist operations; privacy and civil liberties as they relate to electronic communications; data mining; large-scale systems development; software development; Intelligence Community needs as they relate to research and development; and networking and social media".[167]

3.68. The study focused on the bulk collection by the US Government (as opposed to CSPs) of both content and communications data, with particular emphasis on the latter. It extended to the bulk collection of metadata for domestic telephone calls under FISA s215, which had previously been the subject of the PCLOB report referred to above, but also to "*a broader set of activities, including the collection of metadata and contents of foreign telephone calls, emails, and other communications*".

3.69. The NAS Report had no doubt that bulk collection was useful:

> "A key value of bulk collection is its record of past SIGINT that may be relevant to subsequent investigations. If past events become interesting in the present because of new circumstances – such as the identification of a new target, indications that a nonnuclear nation is now pursuing the development of nuclear weapons, discovery that an individual is a terrorist, or emergence of new intelligence-gathering priorities, historical events and the

166 The White House, PPD-28 "Signals Intelligence Activities", January 2014, section 5(d).
167 NAS Report, Preface p vii.

context they provide will be available for analysis only if they were previously collected."[168]

3.70. It also concluded that "*other sources of information might provide a partial substitute for bulk collection in some circumstances*", referring in this regard to targeted collection, to the interrogation of bulk data held by CSPs, and to other intelligence sources and methods. But the NAS was clear that none could be a complete substitute, commenting that:

> "Data retained from targeted SIGINT collection might be a partial substitute if the needed information was in fact collected. Bulk data held by other parties might substitute to some extent, but this relies on those parties retaining the information until it is needed, as well as the ability of intelligence agencies to collect or access it in an efficient and timely fashion. Other intelligence sources and methods might also be able to supply some of the lost information, but the committee was not charged to and did not investigate the full range of such alternatives. Note that these alternatives may introduce their own privacy and civil liberties concerns."[169]

3.71. The NAS Report went on to recommend improved controls on the usage of data collected in bulk, to help enforce privacy protections and facilitate compliance auditing.[170]

(7) Assessment of former intelligence professionals

3.72. William Binney's criticisms of bulk capabilities have commanded widespread attention because, prior to his retirement in 2001, he worked as a technical director at the NSA.

3.73. In evidence to the Joint Bill Committee, he accepted the utility (for example in missing persons investigations) of telephone and ICR records being retained by CSPs for a six-month period so that targeted searches could be addressed to them. But he expressed the view that bulk collection "*applies no intelligence or targeting at the point of collection*" and "*inundates analysts with too much data*", causing them to "*lose focus*". His solution was "*smart collection*": "*a focused disciplined professional selection of meaningful data from the flow around the world*", filtering either at the point of collection or subsequently so as to exclude useless material.

3.74. Mr Binney considered that "*bulk data overcollection from Internet and telephony networks undermines security and has consistently resulted in loss of life in my country and elsewhere, from the 9/11 attacks to date*". Pressed as to why the NSA and GCHQ would have invested so heavily in techniques which were

168 NAS Report, section 4.3 p. 57.
169 NAS Report, section 4.3, pp 57-58.
170 NAS Report, chapter 5: "Controlling Usage of Collected Data".

counter-productive, he referred to what he called an "*incestuous relationship*" between the NSA and large contractors employing ex-NSA personnel.[171]

3.75. Two other witnesses with intelligence backgrounds contradicted the evidence of Mr Binney:

(a) David Wells, a GCHQ intelligence officer from 2005 to 2013 who went on to work for an Australian intelligence agency, drew an analogy with the Google search engine, which he described as itself "*in the business of bulk collection*".[172] He noted that the increase in data volume has been accompanied by an improved ability to ask complex and nuanced questions: the intelligent user, far from being overwhelmed by the comprehensive Google dataset, can generally get an answer "*on the first page, if not in the top result*". In the same way:

> "[W]hile intelligence agencies in the UK and elsewhere have access to more communications data than ever before, by using focused queries and data filters, intelligence analysts only need to retrieve and analyse a small fraction of the overall dataset. As with Google, having more data improves the quality of your results. Intelligence analysts can get the data they need comparatively quickly and efficiently."

This was not to reject the importance of targeted technical surveillance: on the contrary, "*analysis of bulk communications data and focused data collection on 'targets of interest' serve different but complementary purposes*".

(b) Dr David Pepper, Director of GCHQ between 2003 and 2008, stated that Mr Binney's analysis was "*misleading in the current UK context*". He considered (like Mr Wells) that "*the techniques we have developed over many years allow for the effective collection of these large volumes and their targeted analysis*", and stated that "*Mr Binney's proposed approach of targeted collection would make it impossible to work backwards and outwards from the discovery of a new threat to uncover the mesh of past and present communications that reveal the structure of threat networks and the identity of their members*".[173]

3.76. The Review team questioned GCHQ about Mr Binney's observations, and received detailed briefing on the evolution of its selection techniques, analytic techniques (tradecraft) and other methods of managing volume. The risks of "*drowning in data*" are undeniable, and rightly recognised by all concerned. But GCHQ showed us that it:

---

171 Written evidence to Joint Bill Committee, DIP0009 and IPB0161; oral evidence, QQ 234-249.
172 Written evidence to Joint Bill Committee, IPB0166.
173 Evidence to Public Bill Committee, April 2016, IPB71.

(a) operates powerful processing systems (filters), that undertake complex processing and apply sophisticated rules to choose which data to collect and which to reject (or "*defeat*"), both at the point of initial collection and at other stages in the processing chain; and

(b) uses intelligent analytic techniques to use the resultant data as effectively as possible.

We saw no sign that such efforts are counter-productive, or that they result from an over-close relationship with large contractors. On the contrary, it was the evidence of Dr Pepper and Mr Wells that chimed with what we heard consistently from the 55 people we met at GCHQ, including both senior management and analysts with first-hand experience of the operations they were describing, and with what we read in its internal documentation.

3.77. That said, William Binney is plainly correct in his central observation: that operational effectiveness is served by reducing as rapidly as possible the volume of material that it is necessary to analyse. It is important for the efficiency of its operations as well as for reasons of privacy that GCHQ continues to refine its techniques for the focused selection of meaningful data from the flow around the world, a theme to which we revert at 9.23-9.24 below.

(8) Assessments of the European Court of Human Rights

3.78. The lawfulness of bulk interception was considered by the ECtHR in the cases of Weber[174] and *Liberty*,[175] discussed in AQOT 5.32-5.34. The ECtHR in *Weber* commented that so-called "*strategic monitoring*" was not in itself a disproportionate interference with the right to privacy,[176] but was not called upon in either case to evaluate the operational case, and lacked in any event the classified basis for doing so.

3.79. Since AQOT was published in mid-2015, two further cases have been decided by the ECtHR: *Zakharov*[177] (a case on targeted interception, like the earlier *Kennedy*);[178] and *Szabó and Vissy* (2016).[179]

3.80. Both cases resulted in findings of violation: but the ECtHR expressed no doubts as to the utility of bulk powers. Indeed on the contrary, the Court stated in *Szabó and Vissy* that:

174 Application no. 54930/00 *Weber v Germany* (2006).
175 Application no. 58243/00 *Liberty v UK* (2008).
176 At paras 114-117.
177 Application no. 47143/06 *Zakharov v Russia* (2015).
178 Application no. 26839/05 *Kennedy v UK* (2010).
179 Application no. *Szabó and Vissy v Hungary* (2016).

> ".. it is a natural consequence of the forms taken by present-day terrorism that governments resort to cutting-edge technologies in pre-empting such attacks, including the massive monitoring of communications susceptible to containing indications of impending incidents",

and added that "*[t]he techniques applied in such monitoring operations have demonstrated a remarkable progress in recent years*", before emphasising the need for a commensurate development of legal safeguards.[180]

(9) Assessments of the Court of Justice of the European Union

3.81. In the 2014 case of *Digital Rights* Ireland, discussed at length in AQOT 5.63-5.74, the CJEU declared invalid the Data Retention Directive, but was nonetheless prepared to assume that the bulk collection of communications data was of utility. It stated that:

(a) data retained under the Directive was "*a valuable tool for criminal investigations*" which afforded the authorities "*additional opportunities to shed light on serious crime*"; and that

(b) the fight against serious crime was potentially dependent for its effectiveness on "*the use of modern investigation techniques*".[181]

3.82. The value of that assumption is obviously limited, since (like the conclusions of the ECtHR) it was not based on the examination of security-cleared evidence. The scheme under the Directive is in any event not one of the powers under review, though it has similarities with bulk acquisition (2.29-2.45 above). The assumption of the CJEU is however supported by my own conclusions, based on evidence I had seen in the UK and in Germany and on published material: AQOT 14.14-14.22 and Annexes 10-14.

3.83. The legal challenge to DRIPA 2014 brought by David Davis MP and Tom Watson MP (from which the former withdrew on his appointment to the Government) has not yet produced a judgment from the CJEU. But an Advocate General, a member of that court tasked with advising the judges on how they should rule, produced an opinion in July 2016 in which he expressed himself to

---

180 *Ibid.*, para 68. Cf. the approach of the European Commission for Democracy through Law (Venice Commission), which in its report of April 2015 accepted the utility of what it called "*strategic surveillance*", particularly for target development, and stressed the need for strong oversight: AQOT 14.44(b). In its recent report on the Bill, the Joint Committee on Human Rights expressed the view that "*[o]n the current state of the ECHR case-law, we do not consider the bulk powers in the Bill to be inherently incompatible with the right to respect for private life, but capable of being justified if they have a sufficiently clear legal basis, are shown to be necessary, and are proportionate in that they are accompanied by adequate safeguards against arbitrariness*": "Legislative Scrutiny: Investigatory Powers Bill" (HL Paper 6, HC 104, 2 June 2016).

181 Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and others* ECLI:EU:C:2014:238, paras 49 and 51.

be "*clear about the usefulness of general data retention obligations in the fight against serious crime*". That usefulness was said to derive from the capability "*to examine the past by consulting data that retraces the history of communications effected by persons even before they are suspected of being connected with a serious crime*".[182]

(10) Assessment of the SURVEILLE project

3.84. The EU-funded SURVEILLE project was an ambitious attempt, written up in some 40 research papers over more than three years, to develop a matrix of surveillance technologies, scoring them according to the categories of usability, ethics and fundamental (or human) rights. The concept of such a matrix is a potentially useful one, though I have previously referred to some of my own reservations about the project's methodology, informed by a meeting with SURVEILLE staff and external assessors prior to its launch in May 2015.[183]

3.85. SURVEILLE appears to acknowledge that what it referred to (inappositely, in the case of the powers under review) as "*electronic mass surveillance*" is capable of delivering at least some useful results. But it concluded in a synthesis report that the "*medium-level usability scores*" of such techniques were outweighed by high degrees of ethical and legal risk, and contrasted them with the "*clearly higher usability scores*" associated with "*traditional (non-technological) surveillance measures*".[184]

3.86. Any thoughts expressed in SURVEILLE on the absolute and relative effectiveness of covert capabilities were based not on detailed classified inquiries of the kind that the Commissioners, the ISC, my own Reviews and (in the US) the PCLOB and NAS have been able to conduct, nor even on the open conclusions of those inquiries, but rather on what SURVEILLE itself characterises as "*educated guesswork*". If only for that reason, and whatever its other merits, the SURVEILLE project cannot be considered a source of comparable weight for assessing the practical operational case for bulk powers generally, or of the powers under review.

Conclusion

3.87. In summary, and despite the fact that most of the powers under review were first avowed only in 2015, positive statements have been made as to the utility of

---

182 Case C-698/15 *Secretary of State for the Home Department v Tom Watson and others* ECLI:EU:C:2016:572, Opinion of 19 July 2016, paras 178, 181. The case does not relate directly to the powers under review, though the quoted remarks are transferrable to all bulk powers in the broad sense of the phrase: 1.5 above.

183 AQOT p.269 fn 42.

184 SURVEILLE Deliverable D4.10, April 2015, p.15.

each of the four powers under review by security-cleared bodies and individuals as follows:

(a) as to ***bulk interception***, by the IOCC (3.9-3.11 above) and the ISC (3.25-3.26 above);

(b) as to ***bulk acquisition***, by the IOCC (3.12-3.13 above) and in some respects by the IsComm (3.21 above);

(c) as to ***bulk EI***, by the Chair of the ISC, apparently on behalf of other ISC members (3.36 above);[185] and

(d) as to ***BPDs***, by successive IsComms (3.16-3.19) and the ISC (3.32 above).

3.88. The IPT has looked or is looking at all four of the powers under review, but has not so far been called upon to assess the strength of the operational case or to decide whether equivalent results could have been reached by other means.

3.89. Of further relevance are the assessments of the PCLOB in the US (3.43-3.65 above), of the US National Academy of Sciences (3.66-3.71) and of the intelligence professionals who debated the issue in evidence before the Joint Bill Committee and Public Bill Committee (3.72-3.7 above). Despite the contrary opinion of William Binney, I find these assessments to be supportive of the utility of bulk interception, and of little relevance to the bulk acquisition power because of the significant differences between that power and the s215 power in the US.

[185] The ISC also noted the utility of EI, without specific reference to bulk: 3.29, 3.33 above.

4. CRITERIA FOR DETERMINING UTILITY

4.1. The purpose of this chapter is to explain the methodology by which I have sought to evaluate the operational case for the powers under review.

Framework for evaluating outcomes

4.2. The first issue is to identify a class of beneficial outcomes against which the utility of the bulk powers can be measured.

4.3. It will always be relevant to know whether an operation has achieved a tangible beneficial result, such as a conviction or a disruption. But there is a danger that by focusing only on what can be easily measured (arrests, convictions, recruitment of agents) or easily understood (thwarting of a specific planned attack, receipt of valuable information about the intentions of a foreign power), the overall benefits of intelligence work can be understated.

4.4. Anyone who knows intelligence work is aware that many of its benefits come at a relatively early stage in any investigation or operation, before a specific crime is in prospect or the police have become involved.

4.5. A frame of reference is needed for the purposes of evaluating the utility or otherwise of the powers under review. Such a framework is not provided by the Operational Case, which categorises the purposes served by the powers under review in ways which lack coherence and consistency.[186]

4.6. I pointed this out to the SIAs at the outset of the Review, and asked them to agree a classification against which their claims of utility could be evaluated. They responded with a joint document (Annex 4) which sets out what they described as "*a high-level structured description both of the stages of security and intelligence work and the specific activities undertaken within those stages*".

4.7. The three stages of security and intelligence work to which bulk data is said be relevant (though they are not followed in a strictly linear way) were expressed in that document as follows:

> "IDENTIFY
>
> This is the process by which initial '*seed*' information is analysed and developed to the point where it is clear that there is e.g. a potential terrorist threat, a possible candidate for recruitment as an agent, or a source of exploitable intelligence meeting current requirements. The initial '*seed*'

[186] For example, the box on p. 17 presents six purposes for which access to bulk data is said to be essential: but those categories overlap and do not always marry up with the examples given in the specific chapters that follow. On pp. 24-25, two separate classifications of "*Operational Purposes*" are given.

information may come from anywhere: open source (a tweet claiming responsibility for an activity, say); a humint tip-off; forensic data from seized media; information from a foreign liaison partner. Bulk data is vital at this stage in the process and may often be one of the only sources of information available to the Agencies.

UNDERSTAND

This is the process by which the intelligence picture is developed and enriched to the point where decisions can be taken about resourcing and prioritisation. Bulk data is used to help assess potential threats and opportunities, and where appropriate to seek authorisation for targeted intelligence collection to supplement bulk data.

ACTION

This action encompasses a wide range of activities, which bulk data will have helped to inform. The output of the '*identify*' and '*understand*' phases might be the production of intelligence reports, the running of recruitment operations, or the launching of a disruption activity, such as through arrests to prevent a e.g. terrorist attack plan."

4.8. The specific activities conducted by analysts within the SIAs were expressed as follows:

"Target discovery – identifying individuals who may be subjects of intelligence interest from lead intelligence.

Target development – enriching understanding of a subject of intelligence interest, their connections, networks and patterns of activity, in order to understand potential threat or opportunities.

Anomaly detection – a technology-based process by which patterns in bulk data are identified and analysed to assist in the detection of e.g. malware and cyber-attack signatures. This is essential for Cyber Defence.

Network Analysis – this is a technology-based process by which information is gathered from interception to develop understanding of the network environment to provide context to the intercepted data and enable more effective operation of e.g. the bulk interception process.

Triage and prioritisation – at all stages bulk data helps to inform decisions about prioritisation of resources by the Agencies, including the allocation of scarce technical, analytic, human or other collection resources."

4.9. As will be apparent, many of the benefits of intelligence work come at a relatively early stage in the investigative process. Some outcomes may have value even though they do not contribute tangibly to national security (e.g. ruling out a line of enquiry; establishing that a foreign national is not willing to be recruited).

4.10. I have found these classifications to be a useful way of evaluating the claims of utility that have been made to the Review team. They are adopted in the remainder of this Report.

The measure of utility

4.11. Establishing a framework such as that described in the last section is a start. It is then necessary to assess the role of the powers under review in contributing to a beneficial outcome.

4.12. Cause and effect in this area are not always straightforward: indeed it will only rarely be possible to attribute a successful outcome solely to the exercise of a particular power. In almost every scenario to which I have been introduced, both in the course of this Review and in several years of reviewing counter-terrorism operations, various types of intelligence are drawn upon. A mosaic of different information sources is classically involved in identifying a target or threat, developing an understanding of the situation or taking the decision to launch disruptive action.

4.13. It would be unduly simplistic to insist, as a measure of utility, that the exercise of a particular power must have identified or discounted a threat, caused disruptive action to be launched, averted an incident or led to an arrest. Such outcomes will typically be the product of numerous factors.

4.14. For this reason, I have found it more useful to ask not whether a given outcome can be attributed to the use of a bulk power, but rather to think in terms of whether the use of such a power has made a significant contribution to one of the processes or outcomes identified at 4.7-4.8 above.

Assessing alternatives

4.15. My task consists not only of determining whether the use of the powers under review contributed to the positive outcomes claimed, but of asking whether similar results could have been achieved by other, less intrusive, means.

4.16. At one level, this is both feasible and straightforward. On a narrowly-focused, case-by-case basis, it can sensibly be asked whether a particular outcome (e.g. the identification of a threat, the tracing of a person's contacts or the recruitment of an agent in a particular place) could have been achieved by less intrusive means, and I have sought to do so.

4.17. For example, it is legitimate (and necessary) to ask whether:

(a) targeted interception warrants are an adequate alternative to the first of the bulk interception processes described at 2.19(a) above; and whether

(b) the use of data retained by CSPs pursuant to the power in Part 4 of the Bill is an adequate alternative to the data acquisition power.

But the wider the lens, the more imponderables come into the exercise, and the more difficult the assessment.

4.18. For example, it is perfectly legitimate to ask whether the money put into bulk collection and analysis might be more productively spent on different priorities such as hardening domestic targets, or recruiting additional armed or cyber-trained police. But these are decisions of a political and budgetary nature, the answers to which depend upon the cost and efficacy of those alternatives (matters on which I have no evidence), and upon value judgements that are beyond the scope of a report such as this.

4.19. There are, in any event, severe difficulties in comparing such different policies by seeking to attach a financial value to estimates of lives saved, assets seized, children safeguarded, paedophile rings disrupted and so on. Precisely such an approach, in a Home Office impact assessment, was strongly rejected by the parliamentary Joint Committee that considered the draft Communications Data Bill of 2012.[187] The difficulties are especially pronounced in relation to the prevention of terrorism, a type of crime whose worst effects are measured not in production lost or even in lives taken, but in the fear and divided societies which it aims to provoke.

4.20. Accordingly, though I have considered alternative means of achieving specific outcomes to which bulk powers made a significant contribution, I have sought to conduct neither a formal cost-benefit analysis nor a comparison between alternatives that are not readily comparable. That is in accordance with my remit, which asked me to assess whether the same results could have been achieved "*through alternative* ***investigative*** *methods*".[188]

Burden of proof

4.21. The purpose of the Review is neither to advise on the law, nor to replicate or pre-empt any analysis of utility that a court or tribunal may in the future be called upon to perform. Nonetheless, a legal analogy may be helpful in determining the correct approach to the Review's central task.

4.22. The exercise of each of the powers under review is liable to interfere with the right to privacy guaranteed by the Human Rights Act 1998 (which gives effect to

[187] Joint Committee on the Draft Communications Data Bill (HC Paper 79, HC 479, November 2012, paras 264-270.

[188] Annex 3, letter from the Security Minister, para 3.

Article 8 of the ECHR) and the equivalent provisions of EU law.[189] That is because in law, there is an interference not only when material is read, analysed and shared with other authorities,[190] but also when it is collected, stored and filtered, even without human intervention.[191]

4.23. It is, furthermore, the state which in law bears the burden of establishing that any such interference is in accordance with the law, necessary in pursuit of a legitimate aim and proportionate.[192]

4.24. In approaching my task, I have proceeded on the basis of these principles. In particular:

(a) I have not assumed that the powers under review have utility, even when expert security-cleared bodies have previously opined that this is the case.

(b) On the contrary, I have required the Government (including, in particular, the SIAs) to make good from first principles their claims of utility. In lawyers' language, I have put them to strict proof of what they assert.

Sources of evidence: case studies

4.25. In the Operational Case, the Government sought to make the argument for the utility of the powers under review by reference in particular to 19 anonymised (and in some cases, hypothetical) case studies:

(a) three relating to bulk interception (in the fields of counter-terrorism, child sexual exploitation, cyber-defence);

(b) three relating to bulk equipment interference (counter-terrorism, biological weapons proliferation, cyber-defence);

(c) six relating to bulk acquisition (preventing bombings in London and elsewhere in the UK, preventing a kidnap, catching and prosecuting terrorists, thwarting mass casualty attacks against aviation); and

---

189 Article 8 of the ECHR prohibits interference with public authorities with the exercise of the right to respect for private and family life, home and correspondence, save on the conditions set out in Article 8(2): see AQOT 5.16-5.24. See also Articles 7 and 8 of the Charter of Fundamental Rights of the EU. For the central importance of privacy, see AQOT chapter 2.

190 *Weber and Saravia v Germany* (Application no. 54930/00, judgment of 26 June 2006), para 79.

191 The UK Supreme Court has described it as clear that "*the state's systematic collection and storage in retrievable form even of public information about an individual is an interference with private life*": *Catt v Association of Chief Police Officers of England Wales and Northern Ireland and others* [2015] UKSC 9, per Lord Sumption at para 6.

192 This is the "*triple test*" identified in the 2015 ISC Report, paras 23-27. As I noted in AQOT 5.18, the legal boundary between necessity and proportionality is not as clear as that summary suggests: see further 9.3 below.

(d) seven relating to BPDs (focusing investigative resources, stopping terrorist plots, identifying foreign fighters and subjects of interest, preventing terrorist access to firearms, identifying human intelligence agents and protecting major events).

Further details of these, together with an additional eight BPD case studies, were provided to the ISC.

4.26. The Review team was given details of all the real case studies summarised in the Operational Case and material given to the ISC, and discussed with the SIAs hypothetical cases and situations similar to those set out in those documents. In addition we were given 11 further examples of the use of bulk interception, 19 of the use of bulk acquisition, two of thematic EI (bulk EI having not yet been used: 1.19 above) and 17 of the use of BPDs. The case studies examined by the Review team are summarised at Annexes 8-11: some of the numerous BPD case studies were not selected for examination of underlying material or detailed discussion with the SIAs, and have been omitted from Annex 11.

4.27. Assisted by the considerable range of expertise within the Review team, I have evaluated those case studies that were developed to us by the SIAs.

4.28. As a team, we were not content with assertions of utility but insisted on seeing contemporaneous intelligence reports and on interrogating SIA analysts who had actually been involved in the relevant operations.[193] Using the investigative experience available to the Review, we also pursued with the SIAs the possibility that alternative and less intrusive means could have been used to achieve the same result.

Sources of evidence: other

4.29. Well-evidenced case studies demonstrating the successful use of powers under review may be considered *necessary* to establish the utility of those powers. If (hypothetically) the SIAs are unable to show that an existing power has been successfully used, on the basis of the criteria set out above, they will have failed to discharge the burden of establishing the utility of that power.

4.30. To reference a few success stories, even if they are impeccably evidenced and withstand careful scrutiny, is however not *sufficient*. Proof that a power has on occasion been useful is of value: but it is not enough to establish the overall

[193] This was also the approach that I took in relation to the six case studies published in Annex 9 of AQOT, as well as the "*other detailed examples*" relating to bulk interception that I was shown during that earlier review: see AQOT 7.26. It helps explain why we met with as many as 85 SIA officers and staff during the course of the Review: 1.40 above.

utility or necessity of the power. A fully rounded view is likely to depend, in addition, upon:

(a) attempting to evaluate the overall contribution of the powers under review to the objectives for which they were deployed;

(b) looking at failures as well as successes;

(c) asking whether the use of alternative, less intrusive means could have achieved the same (or greater) successes, and avoided some or all of the failures; and

(d) having recourse to assessments of comparable powers, in the UK or elsewhere.

Evidence generated by SIAs

4.31. Those approaches require evidence of a different nature from the intelligence reports and testimony of analysts which informed our approach to the case studies. They have caused us, in particular, to ask the SIAs for details of:

(a) how often the powers under review are used;

(b) negative incidents and outcomes associated with the use of the powers under review;

(c) the criteria applied internally to assess the utility of the powers;

(d) evidence in support of applications for renewal of bulk warrants, funding etc.; and

(e) internal documents considering the utility of the powers under review, both in absolute terms and relative to other priorities.

4.32. The last category of documents has the potential to be particularly valuable, since it includes documents that were produced not for the purposes of achieving a beneficial outcome for a SIA (e.g. a funding increase, or the renewal of a warrant), but to assist internal reflection and the setting of corporate priorities. Where such documents were prepared in a spirit of open-minded discussion or enquiry, it is harder to dismiss them as one-sided or self-serving.

4.33. My request for full disclosure of such documents (specifically including any that were unhelpful to the SIAs' case) was said to be unprecedented. But the SIAs complied willingly. A large quantity of documentation was handed over in short order. No attempt was made to redact this material, despite its highly sensitive nature and some references in it to shortcomings, unintended consequences and

lack of success.[194] We took this as a sign that the SIAs were dealing frankly with us – and also of their confidence that, viewed overall, the story they had to tell was a positive one.

Historical and comparative usage

4.34. I also considered, more briefly, the ***history*** of each of the powers under review, and the extent to which it has been used by ***bodies other than the SIA***, both in the UK and abroad. Such use by others is of course not directly probative of practical utility, any more than is use by the SIAs themselves. But to the extent that others may (or may not) have troubled to develop and deploy such powers, that fact may be an indicator of their utility and necessity.

Snowden documents

4.35. I have also had regard to the Snowden documents. Despite the fact that for the most part their contents have been neither confirmed nor denied **[NCND]** by the Government, I have had the opportunity to question the Government privately on various matters referred to in that material, and have received a number of detailed briefings.

Previous reviews

4.36. Last but not least, I thought it important to take on board the conclusions of the other bodies which have considered the utility of the powers under review, or similar powers – particularly those whose assessment has been informed by detailed access to the classified detail.

4.37. Relevant in that regard are the various reports and studies referred to in chapter 3, above. Where I have been unsure of the significance of their findings, I have engaged where possible with those responsible in order to improve my understanding of their conclusions.

Conclusion

4.38. None of these approaches, or classes of evidence, could be determinative on its own of the issues I am asked to consider. Some may offer no more than a glancing or peripheral insight. But by coming at the issue from a number of different angles, it has been possible to arrive at conclusions that I have felt able to state with a high degree of confidence.

[194] See e.g. 7.24-7.25 below, on EI.

5. ASSESSMENT: BULK INTERCEPTION

Claimed utility

5.1. The bulk interception power is currently exercised only by GCHQ, and we understand that this is not likely to change.[195]

5.2. Cathryn McGahey QC and I have inspected a great deal of closed material concerning the value of bulk interception, including warrant renewal applications (which contain details of the use to which intelligence derived from bulk interception had been put) and explanations produced for the benefit of the ISC and the Review.

5.3. The value of bulk interception is summarised on an open basis in the Operational Case (7.1-7.2) as follows:

> "Bulk interception is a capability designed to obtain foreign-focused intelligence and identify individuals, groups and organisations overseas that pose a threat to the UK. It allows the security and intelligence agencies to intercept the communications of individuals outside the UK and then filter and analyse that material in order to identify communications of intelligence value.
>
> Bulk interception is essential because the security and intelligence agencies frequently have only small fragments of intelligence or early, unformed, leads about people overseas who pose a threat to the UK. Equally, terrorists, criminals and hostile foreign intelligence services are increasingly sophisticated at evading detection by traditional means. Just as importantly, due to the nature of the global internet, the route a particular communication will travel is hugely unpredictable. Combined, this means that sometimes the data acquired via bulk interception is the only way the security and intelligence agencies can gain insight into particular areas and threats. Access to large volumes of data is therefore essential to enable communications relating to subjects of interest to be identified and subsequently pieced together in the course of an investigation."

5.4. A more detailed statement of the utility of bulk interception, arranged by reference to the SIAs' agreed structured description of security and intelligence work,[196] was supplied to the Review by GCHQ (Annex 7).[197] In summary:

(a) GCHQ described its ability to interrogate the communications data obtained through bulk interception as providing "*the key capability to answer questions about developing incidents as they occur and identify the individuals involved*".

---

195 See further 2.6-2.28 above.

196 4.2-4.10 above and Annex 4.

197 I leave out of account those parts of this document that refer to the advantages to be gained from *interception generally*, rather than *bulk interception* (e.g. the citation from Charles Farr's witness statement under the heading Understand).

(b) The utility of the bulk powers (including bulk interception) was said to be "*the same across the majority of GCHQ's operational areas*", including economic security, weapons and counter-proliferation, serious crime, cyber defence and counter-terrorism.

(c) Cyber-defence was given particular emphasis: GCHQ state that 95% of the cyber-attacks on the UK detected by the SIAs in the first half of 2016 were only discovered through the collection and analysis of communications data obtained through bulk interception.

(d) The value of bulk interception was said to be constant where cyber-defence is concerned, and to be constant or declining in other respects.

5.5. Recalling the ISC's comment that "*the primary value to GCHQ of bulk interception was not in reading the actual content of communications*",[198] no specific mention was made in GCHQ's statement of utility of the value (if any) attached to content obtained by use of bulk interception. This raises the question of whether it is necessary for bulk interception warrants to permit the recovery of content at all. I was assured that it did, in two respects:

(a) The initial recovery of communications data may be used as "*building block*" information to assist in determining whether to access content under the same warrant; and

(b) The process described at 2.19(b) above allows content-based criteria (for example, the use of complex criteria with three or more elements that is used to identify individuals possibly breaching UN sanctions) for selecting communication items for analysis.

5.6. GCHQ emphasised, in discussions with members of the Review team, that its ability to provide speedy information on incidents as they were occurring depended on its ability to interrogate the communications data obtained through the process described at 2.19(b) above.

5.7. MI6 records in its own statement of utility (Annex 6) that it depends on GCHQ's use of bulk interception to provide targeted information that it can then develop to understand intelligence threats and opportunities. Without this, it claims that its "*operations across all areas (counter-terrorism, counter-proliferation, cyber, serious crime and geographical requirements for intelligence collection) would be significantly damaged, including the ability to understand operational risks and manage them appropriately*".

[198] 2015 ISC Report, para 80; 3.26 above.

Scale of use

5.8. Neither MI5 nor MI6 conducts bulk interception, or envisages doing so, though both use its intelligence product in their operations. For the foreseeable future, all use of the interception power is likely therefore to be by GCHQ.

5.9. We were told that just under half of all GCHQ intelligence reporting is based on data obtained under bulk interception warrants. For counter-terrorism intelligence reporting, this figure rises to over half.

5.10. It is said that to break these approximate figures down further would damage national security by revealing too much about GCHQ's capabilities. But I can confirm that (as indicated at 5.5-5.6 above):

(a) each of the collection methods summarised at 2.19 above made a significant contribution to GCHQ's intelligence effort; and that

(b) the content of communications (and not simply secondary data) may be crucial to identifying the intentions and plans of individuals. Six of the case studies annexed to this Report involved the use of content (5.18 below), and two thirds of GCHQ's highest grate reporting from intercepted material is based on content.[199]

5.11. Having inspected a good number of intelligence reports and internal documents (as to which, see further below), I have no doubt that the bulk interception power continues to be used productively and on a large scale by GCHQ.

Case studies (Annex 8)[200]

5.12. At the Review team's principal meeting with GCHQ, we were provided with details of nine case studies relating to bulk interception, (A8/1,3-10). We were able to view underlying contemporary documents in relation to those case studies, and to question analysts and managers with knowledge of those operations. Subsequently, the Review team was provided with a further four case studies (A8/2,11-13). The Review team did not have the opportunity to discuss these case studies with those involved in the operations, nor to view documents relating to them. I had, though, been given details of two of these

199 GCHQ's highest-grade reporting contains intelligence that could change UK government policy, fill in details of a threat to life situation or provide highly important operational information, such as that which might keep an agent safe. To meet this threshold, it is usually the meaning of the communication rather than the fact of its existence that would provide the crucial intelligence.

200 For convenience I refer (for example) to Case Study 5 in Annex 8 to this Report as A8/5.

operations (A8/2,11) during my work on *A Question of Trust*[201], and Cathryn McGahey QC had detailed knowledge of one of these (A8/2) from previous work.

5.13. A8/5 and A8/10 had featured in the Operational Case: the Review team was also given (A8/8) an example of the cyber-defence work described in more general terms as a case study in the Operational Case.

5.14. In addition, GCHQ provided samples of intelligence reports which were graded as being highly valuable and which contained intelligence obtained through bulk interception of content.

5.15. The case studies illustrated the use of bulk interception in a wide range of fields, including counter-terrorism in the UK and overseas (A8/1-5), cyber-defence (A8/8-9), child sexual exploitation (A8/10-11) and organised crime (A8/12-13). We were also given extensive detail of GCHQ's work to support military operations (A8/6-7).

5.16. The case studies illustrated the value of bulk interception in target discovery and development (e.g. A8/2,3). A8/2 involved the analysis of patterns of behaviour to identify terrorists. A8/3 showed the use of bulk interception at substantial scale; both communications data and content obtained through bulk interception were used to triage some 1,600 leads provided to the SIAs in the wake of attacks in France.

5.17. However, the predominant use of bulk interception, at least in the examples given to the Review team, was as the basis for action, frequently with other SIAs or the police. For example:

(a) GCHQ used bulk interception of communications data to identify individuals planning a terrorist attack against the UK; the intelligence was passed to the police, who were able to prevent an attack from taking place (A8/1).

(b) The use of intelligence gained through bulk interception as a basis for urgent action was illustrated starkly in the case of a kidnapping in Afghanistan (A8/6). Bulk interception of communications data led to hostages being located within 72 hours of their abduction; bulk interception of content revealed an immediate threat to the life of the hostages, and to an urgent (and successful) military rescue mission.

5.18. The case studies indicate that, whilst substantially more use is made of communications data than of content, content is often crucial to uncovering the

[201] AQOT Annex 9 Case Study 5

intentions and plans of individuals in a way that could not be achieved with only communications data.[202] Thus:

(a) A8/4 and 8-13 involved the selection for examination of intercepted communications data alone.

(b) A8/1-3 and 5-7 involved the examination of both communications data and content obtained through bulk interception. In some of these instances (e.g. A8/6-7), content was intercepted *after* the relevant telephone or email address had been identified through the interrogation of bulk secondary data.

5.19. No case study shown to the Review team involved the use of bulk interception of content alone. GCHQ told me that *"secondary data will almost always have been crucial in ensuring that content was available to the analyst to report".*

Alternative methods

5.20. During the presentation by GCHQ of the case studies, members of the Review team questioned the decision in each case to use bulk interception and explored alternatives.

5.21. Potential alternatives inevitably varied with the nature of each case but the Review team looked in particular at targeted interception and the use of human sources. In cyber-crime, the use of commercial cyber-defence products was considered.[203]

Targeted interception

5.22. In the case of bulk interception based on a strong selector (described in para. 2.19(a) above), it might appear that a targeted warrant would be a viable alternative; the selector is after all already known.

5.23. A similar point could be made in those instances in which the relevant device or email address had first been identified through the interrogation of bulk secondary data (A8/6-7). The interception of content was authorised under the terms of the bulk interception warrant used to obtain the secondary data; but we pressed GCHQ on why, having obtained the secondary data, it could not have applied for a targeted warrant to obtain content.[204]

---

202 For example, in the Afghan hostage case study (A8/6), there would have been no way to know that the hostages were in imminent danger using communications data alone.

203 Liberty suggested (Submission of 31 July 2016, para 30) that targeted EI could be another alternative. But even if the target is known, the conditions for the use of targeted EI will not always be satisfied.

204 Cf. AQOT, Recommendation 80(a).

5.24. GCHQ explained in response that, in very many instances, a targeted warrant would not produce the same result in an overseas context. In particular:

(a) The location of some targets (e.g. A8/6-7) means that targeted interception would not be practicable.

(b) Even in more favourable overseas locations, the cooperation of local CSPs in giving effect to a targeted warrant might not be forthcoming, or might be possible only after delays.

(c) The fragmentary nature of global communications, involving the division of communications into packets, meant that a targeted warrant would not, or not necessarily, capture all the information that GCHQ needed.

(d) The number of overseas targets could render such a regime prohibitively cumbersome.

5.25. Problems of delay and co-operation (5.24(b) above) would certainly have faced those seeking to triage 1,600 leads after terrorist attacks in France (A8/3). Even assuming that overseas CSPs had retained the necessary data and were willing to co-operate,[205] it would clearly have taken a substantial time to obtain, through targeted means, intelligence on such a scale. The operation was being conducted at a time at which there was an urgent need to identify imminent threats.

5.26. In the case of the Afghanistan hostages, I concluded that without the use of bulk interception, it was highly likely that one or more hostages would have been killed before a rescue could be attempted.

5.27. For these reasons, I was not persuaded that a targeted warrant would be an adequate alternative for the gathering of content overseas in cases where a strong selector is already known.

5.28. In its submission to the Review of 31 July 2016, Liberty analysed the bulk interception case studies in the open Operational Case and argued that, in the case of the first two (A8/5,10), targeted interception would have provided a satisfactory alternative. In respect of A8/5, Liberty contended that the identification of terrorist connections ("*contact chaining*") could be achieved through interrogation of data obtained through targeted means, which would lead to "*the discovery of valuable targets and the rapid onset of further collection on newly discovered targets*".

[205] See 5.34, below

5.29. As I noted at 1.48 above, Liberty had the disadvantage of having only the very limited information made public in the open Operational Case. Eric King, who also commented on the document, made the point that there was insufficient information in that document for meaningful criticism or analysis of A8/5 to be possible.

5.30. I was able to consider each case study in considerably more detail, and with the help of Cathryn McGahey QC and Gordon Meldrum, carefully examined possible alternatives in these and all other case studies.

5.31. Contact chaining, using data already acquired in respect of targets likely to be linked to a subject of interest, is undoubtedly a valuable technique. But equally plainly, it has limitations. In particular:

(a) Contact chaining depends upon:

- the SIAs already knowing their initial subject of interest,
- new subjects of interest being in contact with the initial subject, and
- it being possible to serve a targeted interception warrant on the new subjects.

These conditions will not always be satisfied (particularly, in the case of the third, in the overseas context): bulk interception offers other routes by which new contacts can be discovered.

(b) The purpose of contact chaining is to find additional contacts who use the same form of communication. But bulk interception may allow GCHQ to find additional forms of communication between subjects of interest.

5.32. In A8/5, the extremists were using a variety of different communications methods in an effort to conceal their activities (a detail not set out in the open Operational Case). Contact chaining would not have led to the identification of the unknown email address. I am satisfied that, without bulk interception, it is very unlikely that this email address and its user would have been identified.

5.33. In respect of A8/10, bulk interception was used to identify an individual who was taking great care to conceal his identity online, while engaging in child sexual exploitation. GCHQ accepted that some of the results obtained through the use of bulk interception could have been achieved through requesting targeted data from CSPs in the UK and abroad. But GCHQ told me, and I accept, that these sources tend to provide less complete information and are less satisfactory as a means of identifying individuals who take sophisticated measures to avoid

detection. Further, when working with CSPs overseas, GCHQ is entirely reliant on the cooperation of those CSPs.[206]

Bulk acquisition

5.34. Where communications data are concerned, bulk acquisition could in some circumstances be an adequate alternative to bulk interception: but it would not be noticeably less intrusive and would have a disadvantage in terms of speed, amongst other concerns. We were told that it may take some time to persuade an overseas service provider to cooperate, and some may not co-operate at all. Most communications with overseas CSPs have to be made through foreign intelligence partners, causing further delays. It may not be possible safely to serve a national security-related warrant on an overseas CSP; and the CSP may not hold the range of data required.[207]

Human sources

5.35. In other instances examined by the Review team, potential alternatives were unavailable or carried their own risks. It might, for example, in the case of threats to Camp Bastion (A8/7), have been theoretically possible to seek information about such threats from a human agent, assuming that one had been available. However, the obvious dangers to agents and their handlers, whether acting in volatile situations overseas or working to counter terrorism at home, must also be taken into account.

Commercial cyber-defence products

5.36. In the field of cyber-crime, there are undoubtedly commercial providers who offer products to defend against cyber-attack. But only those customers who choose to buy those products receive that protection. Case study A8/8 illustrates the advantages that GCHQ has, through its use of bulk interception, in being able to give victims advance warning of an attack. Further, GCHQ, unlike commercial providers, can assess – and take measures against – the threat to the UK in general, and not simply to specific customers.

5.37. In its submission to me of July 2016, Liberty asserted that robust defence of critical networks would be more appropriate than the use of bulk interception. It argued that national cyber-security relied on "*secure online platforms protected by strong encryption; the promotion of industry-wide security standards; trust in UK software, internet and communications service providers; public education in*

206 See further, 5.34 below

207 As in A8/6: a hostage-taking in which bulk interception of communications data led to the hostages being located relatively speedily.

online safety; and effective law enforcement concerning criminals who operate online".

5.38. All the factors identified by Liberty have a role to play in cyber-defence. But none of them, alone or in combination, was able to prevent the cyber-attack described in A8/8, despite the fact that financial institutions had already identified the threat posed by the sophisticated malware concerned. Analysis of bulk interception data available to GCHQ was able to locate that malware on a nationally important computer network.

No possible alternatives

5.39. Some of the case studies demonstrated that no alternative method at all existed of obtaining the necessary intelligence. A8/1 is such an example; faced with an attack plot and no other leads to follow, the SIAs had to rely on bulk interception of communications data to identify those involved. That case study also provides an instance of the utility of different bulk powers in combination: in that case, bulk interception and bulk acquisition of telephone data.

5.40. A8/2 is an example of the use of pattern analysis to identify members of an Islamist extremist cell who would not otherwise have been discovered. Although I cannot publish further details of the operation, I am aware that a very real threat of a mass casualty attack was averted.

5.41. I am conscious that I have seen only a small sample of the SIAs' work, and that one cannot conclude on the basis of such a sample that alternative methods of evidence-gathering would never be available or appropriate. There are circumstances in which they certainly would. However, some of the disadvantages of other methods illustrated by the case studies (such as the risk to human agents or the delay involved in asking overseas CSPs for assistance) are evident. It does not seem to me that any alternative or combination of alternatives would be sufficient to substitute for the bulk interception power.

Negative incidents and outcomes

5.42. IOCCO is under a statutory duty to report to the Prime Minister any contravention of the provisions of RIPA 2000, or any inadequate discharge of the safeguards provided in its s15.[208] A detailed account of interception errors (targeted and bulk) is given in the IOCC's regular published reports: in 2013 there were 57 errors and in 2014 there were 60.[209] The great majority involved technical or human error within interception agencies or CSPs, resulting for example in over-collection, unauthorised disclosure, incorrect dissemination, failure to cancel

208 RIPA 2000, ss58(2)(3).
209 Report of the IOCC, March 2015, 6.86.

interception and the interception of an incorrect communications address. In one very serious incident in 2014, an individual who deliberately undertook a number of unauthorised searches for related communications data had his employment terminated and vetting status withdrawn. But none of the errors was of such a nature as to throw into doubt the utility of the bulk interception power. Nor were they suggestive of an unduly casual approach: the IOCC, while noting that there was room for improvement, spoke of the SIAs' "*strong culture of compliance and of self-reporting when things go wrong*".[210]

5.43. The SIAs make little attempt precisely to assess the extent to which the use of bulk interception achieves or fails to achieve the desired goal. Managers from all SIAs emphasised that, if an analyst's search does not provide the required answers, then further searches will be conducted until success is achieved. It was said to be very rare for any outcome to be achieved through the use of bulk powers (or any one bulk power) alone. Success rates were therefore difficult to measure. I had the impression that the utility of bulk interception may have seemed so self-evident to the SIAs that they had not seen a need to assess its value or failure rate.

Internal documents

5.44. At the outset of the Review I expressed a wish (as noted at 1.34 and 4.32-4.33 above) to see documents internal to the SIAs, including documents prepared for the purposes of frank internal reflection rather than the achievement of a desired outcome such as a funding increase or the grant of a warrant.

5.45. In relation to bulk interception, the Review team was shown a substantial quantity of GCHQ documents, some going back to 2003. These documents provided me with an overview of the development of bulk interception, with an initial focus on content, subsequently broadened to include communications data.

5.46. Among other documents, we saw a series of annual and quarterly performance reports, intended for internal use. Those reports show that bulk interception was seen within GCHQ as underpinning much of its successful work. Bulk interception remained of value, despite the increasing use of encryption, and was noted to be particularly important in enabling target discovery and in pattern analysis.

5.47. Another document, which admittedly (and as GCHQ pointed out to us) was created in November 2015 for submission during a spending round, corroborated what we had heard from front-line analysts about the advantages of bulk

[210] *Ibid.*, p.42.

interception. Entitled "The Value of Bulk Passive", it contained the following summary:

> "*Bulk [interception] also gives us the ability, and flexibility, to detect target use of new technologies and find alternative selectors ... If we didn't have this, we'd be limited to basic contact chaining, which would restrict us to operating in the domain of the original selector ... and we'd not be able to tell whether new technologies were of interest.*"

5.48. The same document identified bulk interception as being "*critical*" for work that required retrospective analysis, was urgent or time-bounded, and for detection work that was based on the use of a technology or on patterns of behaviour or movement. The author recognised that CNE would in future be far more broadly deployed than it was at present, but expressed the view that bulk interception would continue to be pivotal to the success of CNE: it was the use of bulk interception that provided the basic understanding of the system which could then be targeted by CNE.

5.49. A number of recent papers expressed the view that bulk interception remained valuable despite the "*significant threat to the value of bulk passive*" that was posed by the increased use of encryption. The documents overall indicate that GCHQ's public warnings about the "*going dark*" threat accurately reflect its private thoughts; but also that it perceives bulk interception as retaining a significant value, particularly in combination with CNE (or EI) and other techniques.

Conclusion

5.50. I concluded in AQOT, in relation to bulk interception, that:

> "its utility, particularly in fighting terrorism in the years since the London bombings of 2005, has been made clear to me through the presentation of case studies and contemporaneous documents on which I have had the ability to interrogate analysts and other GCHQ staff."[211]

5.51. Outlines of six of the dozen case studies on which I based that conclusion were annexed to AQOT,[212] including three in which exercise of the power by GCHQ led to arrests or the prevention of an attack in other countries. Though it was possible to cite those case studies only in outline, they illustrate in particular the ability of bulk data to identify previously unknown perpetrators of suspicious activity. As I stated in AQOT 7.27: "*They leave me in not the slightest doubt that bulk interception, as it is currently practised, has a valuable role to play in protecting national security*."

---

211 AQOT (June 2015), 14.45.

212 AQOT, Annex 9 (para 1 of that Annex was included in error).

5.52. Those conclusions were in line with those that have been reached by the IOCC and the ISC: 3.87(a) above. Insofar as they relate (at least) to the "*strong selector*" process described at 2.19(a) above, they are in line also with the conclusions of the PCLOB on the analogous s702 power. They further conform to the assessment of former intelligence professionals whose experience is more recent and more UK-focused than that of William Binney (who I accept takes a different view): 3.72-3.77 above.

5.53. This Review has given me the opportunity to revisit my earlier conclusion with the help of Review team members skilled respectively in technology, in complex investigations and in the interrogation of intelligence personnel, and on the basis of considerably more evidence: notably, a variety of well-evidenced case studies, internal documentation and the statistic that almost half of GCHQ's intelligence reporting is based on data obtained under bulk intelligence warrants.

5.54. My opinion can be summarised as follows:

(a) The bulk interception power has proven itself to be of vital utility across the range of GCHQ's operational areas, including counter-terrorism in the UK and abroad, cyber-defence, child sexual exploitation, organised crime and the support of military operations.

(b) The power has been of value in target discovery but also in target development, the triaging of leads and as a basis for disruptive action. It has played an important part, for example, in the prevention of bomb attacks, the rescue of a hostage and the thwarting of numerous cyber-attacks.

(c) While the principal value of the power lies in the collection of secondary data, the collection and analysis of content have also been of very great utility, particularly in assessing the intentions and plans of targets, sometimes in crucial situations.

(d) The various suggested alternatives, alone or in combination, may be useful in individual cases but fall short of matching the results that can be achieved using the bulk interception capability. They may also be slower, more expensive, more intrusive or riskier to life

5.55. All that said, there are signs that outside the field of cyber-defence, where bulk interception is of crucial importance (5.4(c) above), trends towards universal encryption and the anonymisation of devices may be making the bulk interception power into a (gently) diminishing asset. The need for future decision-makers in this field to be fully apprised of the technical picture is addressed, in the context of each of the powers under review, at 9.16-9.32 below.

6. ASSESSMENT: BULK ACQUISITION

Claimed utility

6.1. Cathryn McGahey QC and I inspected a good deal of classified material relating to the utility of the bulk acquisition power, which has been used since at least 2001 by GCHQ and since 2005 by MI5.[213] This material includes the most recent letter to the Secretary of State in which MI5 sought continued authorisation to use the capability (June 2016), which was supported by case studies and in which bulk acquisition was said to provide "*a broad spectrum of intelligence, with greater precision, speed, and often with less intrusion than other tools and techniques*".

6.2. The Operational Case describes access to bulk communications data as "*essential to the security and intelligence agencies in pursuing their investigations*", and puts the case for the bulk acquisition power as follows (at 9.3):

> "Bulk communications data enables the security and intelligence agencies to identify and investigate potential threats in complex and fast-moving investigations. It allows the security and intelligence agencies to conduct more sophisticated analysis, by 'joining the dots' between individuals involved in planning attacks, often working from fragments of intelligence obtained about potential attacks:
>
> - Carefully directed searches of bulk communications data in complex investigations and operations can identify frequent contact between subjects of interest and their associates, including potential attack planning activity.
>
> - Identifying those links between individuals or groups can help to direct where a warrant for more intrusive acquisition of data, such as interception, is needed.
>
> - Bulk communications data allows searches to be conducted for traces of activity by previously unknown suspects who surface in the course of an investigation, helping to identify further potential threats that require investigation."

6.3. Anticipating the counter-argument that there is an adequate alternative in the power to address requests to CSPs who will themselves have retained similar communications data pursuant to Part 4 of the Bill (currently DRIPA 2014), the Operational Case claims for the bulk acquisition power (at 9.4-9.6) the triple advantages of:

---

[213] See further 2.29-2.45 above.

(a) ***ability to perform complex analysis***: "*While the security and intelligence agencies can also make individual communications data requests to communication service providers, the ability to access data in bulk is critical, because it enables the security and intelligence agencies to conduct searches, where necessary and proportionate, across all the relevant data, in a secure way. This enables more complex analysis to be undertaken, particularly when the results are matched against other data holdings – for example, that held in bulk personal datasets*";[214]

(b) ***greater speed***: "*By using bulk communications data, links can be established that would be impossible or significantly slower (potentially taking many days) to discover through a series of individual requests to communication service providers. This can sometimes be the difference between identifying and disrupting a plot, and an attack taking place*"; and

(c) ***lesser intrusiveness***: "*Without access to bulk communications data, the security and intelligence agencies would be much less able to concentrate their efforts on those who pose the greatest threat, and without the benefit of this insight there would be a significantly greater risk of intruding into the lives of innocent individuals during the course of investigations as the security and intelligence agencies work to narrow down possible suspects*."

6.4. MI5's statement of utility (Annex 5) identifies the utility of communications data acquired under the bulk acquisition power, and/or BPD, for identifying (and ruling out) links to known targets and activities of interest, for understanding target behaviour, target communications, travel patterns and links between plotters, for identifying new communications devices that may be subject to further targeted enquiries, for keeping human sources safe and for enabling MI5 and the police to take disruptive action and stop attacks, e.g. by alerting them to changes in behaviour that might indicate the imminence of a terrorist attack. MI5 told the review team that it relied upon bulk acquisition data in its counter-terrorism operations in particular, but also used it in other areas of its work.

6.5. GCHQ in its own statement of utility (Annex 7) describes the bulk acquisition power as "*the primary way in which GCHQ discovers new threats to the UK*", together with communications data obtained through bulk interception. The use of the bulk acquisition power by its geo-political teams "*allow it to minimise intrusion into privacy when seeking to identify new leads*" and can provide assurance that "*an account targeted for more intrusive content collection does not belong to a UK individual*".

214 Cf. Report of the IOCC, July 2016, para 8.29.

6.6. GCHQ uses bulk communications data currently acquired under s94 across the full range of its operational work. It considers s94 data to provide a more reliable and comprehensive feed of particular types of communications data than may be obtained from GCHQ's bulk interception: by merging s94 data with its other communications data holdings, it can use them in a complementary fashion. GCHQ also told us that bulk acquisition was less useful than bulk interception for overseas operations, because it relied on the cooperation of overseas CSPs.[215]

6.7. MI6 stated that it depends on GCHQ's and MI5's use of bulk acquisition to develop its understanding of a threat to the UK, which it can then use its assets and capabilities to inform and disrupt.

6.8. According to GCHQ, the importance of the bulk acquisition power was likely to remain the same or decline. MI5 and MI6 thought it would continue to be important.

Scale of use

6.9. MI6 makes no use of the bulk acquisition power. As IOCCO reported in July 2016, only GCHQ and MI5 had s94 directions to acquire bulk communications data.[216] There is no reason to suppose that this will change once the new power enters into force.

6.10. The Government's claim that the bulk acquisition power is currently used "*on a daily basis*"[217] is borne out in striking fashion by the figures in the recent IOCCO report. IOCCO was satisfied that GCHQ analysts had "*justified properly why it was necessary and proportionate to access the communications data*", and that MI5's applications "*were submitted to an excellent standard and satisfied the principles of necessity and proportionality*".[218] But heavy use was made of the acquired data:

(a) "*In 2015 GCHQ identified 141,251 communications addresses or identifiers of interest from communications data obtained in bulk pursuant to section 94 directions which directly contributed to an intelligence report*."[219]

(b) "*In 2015 the Security Service [MI5] made 20,042 applications to access communications data obtained pursuant to section 94 directions. These applications related to 122,579 items of communications data*."[220]

215 See further 5.34 above
216 IOCCO Report of July 2016, 7.4.
217 Operational Case, 9.1.
218 IOCCO Report of July 2016, 8.62 and 8.70.
219 IOCCO Report of July 2016, 8.62.

We are unfortunately not able to shed further light in an open document on the reasons why such high numbers of applications are recorded.

6.11. More readily comprehensible is the statistic that approximately 5% of GCHQ's intelligence reporting each year contains material from at least one s94 source. The majority of those reports are related to counter-terrorism, with other major areas including serious crime and certain geo-political reporting.

Case studies (Annex 9)

6.12. The case studies are summarised at Annex 9. MI5 provided the Review team with written details of 25 cases. MI5 managers and analysts then gave a presentation to the team, and supplied contemporaneous documents. The team members were able to question staff who were familiar with the operations described in the case studies.

6.13. All the case studies relating to the use of bulk acquisition were provided by MI5, although in A8/1 GCHQ provided an example of the combined use of bulk interception and communications data. The case studies concerned principally Islamist extremist activity in the UK and abroad, and dissident republican activity in Northern Ireland.

6.14. The cases provide illustrations of all three of the *Identify, Understand, Action* categories described by the SIAs (and set out in chapter 4 above). However, the majority of the cases concerned the earlier stages of operations – generally the *Identify* and *Understand* stages, involving target identification and development. This pattern reflected the view given to the Review team by MI5 managers that the use of bulk acquisition (and bulk powers in general) was most valuable at the triaging stage, in order to establish the identity of an individual. We were told that at the stage at which action was required, for example to disrupt a terrorist threat, resources would always be found to take that action. If bulk powers were not available, then other means would be used. However, in the view of MI5 managers, the use of bulk powers was crucial in swiftly obtaining the knowledge necessary for action to be taken.

6.15. Seven of the case studies (A9/1-7) involved the use of bulk acquisition to identify a person of interest. In three of those cases (A9/1,3,4) a real terrorist threat to the UK was identified and steps taken to mitigate that threat. In two others, MI5 identified and was able to counter a threat of espionage (A9/5,7).

---

220 *Ibid.*, 8.70. Some 20,000 applications produced more than 120,000 items of communications data because a single application may request several items of data relating, for example, to a target's telephone number.

6.16. Of the remaining two identification cases:

(a) Interrogation of communications data obtained by bulk acquisition swiftly revealed in one (A9/2) that the person behind a threat was a known hoaxer.

(b) In the other (A9/6), an individual, once identified, was assessed not to pose a threat.

There is a clear value in the use of bulk powers to eliminate lines of enquiry, so that resources can be concentrated elsewhere and disruption to the public minimised.

6.17. A9/8-16 illustrate the *Understand* category of SIA activity. All these case studies concerned Islamist extremist activity in the UK and, to a lesser extent, overseas. In each case, bulk acquisition was used by MI5 to learn more about the activities and plans of an individual or group. Inevitably, there is an overlap between the *Understand* and *Action* categories; in many cases, the understanding gained by MI5 led it, itself or with partners, to take action. A9/10 demonstrates the overlap; in this case, MI5 was able, using bulk acquisition data, swiftly to learn more about the individuals responsible for the failed attacks in London and the attack on Glasgow airport in 2007; MI5 was then, using this intelligence, able to support the police in responding to the attacks and to the threat of further attack.

6.18. A9/17-25 are examples of action being taken to counter Islamist extremist activity, dissident Irish republican threats, weapons proliferation and espionage. Again, there was often no clear dividing line between the categories of *Identify, Understand* and *Action.* Frequently, and as one would expect, one led swiftly to another. Many of these case studies (and some of those placed in the *Understand* category e.g. A9/10-12) involved cases in which individuals were prosecuted. It would be wrong to say in any of these cases that it was only through the use of bulk acquisition data that prosecution became possible: as the SIAs emphasised repeatedly, most operations involve a combination of intelligence-gathering techniques, and the police involvement in the obtaining of admissible evidence is crucial. It can, though, be said that the use of bulk acquisition played a significant role in the cases shown to us in which prosecution followed.

6.19. The case studies demonstrate that bulk acquisition provides MI5 with a valuable means to obtain intelligence quickly. GCHQ told the Review team that bulk acquisition was generally not a viable alternative to bulk interception for overseas operations, because GCHQ would have to rely on the co-operation of overseas CSPs.[221] In MI5's UK-based operations, the same disadvantage in the use of

[221] See further, 5.34 above.

bulk acquisition does not exist. The data may be readily obtained and swiftly analysed.

6.20. The case studies also indicate that bulk acquisition data is used by MI5 to enable it to focus and prioritise targeted techniques. Case study 4 provides an illustration: bulk acquisition was used to identify an individual in contact with a senior Islamist extremist. More intrusive, targeted techniques were then used against that individual in order to assess the threat, if any, posed to the UK.

6.21. I understand that GCHQ merges the bulk acquisition data in its possession with bulk interception data, and that GCHQ analysts conducting searches will not necessarily be aware of the source of the information that they obtain. A8/1 was the only example provided by GCHQ of its use of bulk acquisition.

Alternative methods

6.22. The Review team questioned MI5 staff about the availability of alternatives, both by reference to the case studies and more generally. We considered, in particular, the use of the DRIPA power (2.33 above), to be replaced by similar provisions of the Bill under which CSPs can be required to retain communications data (Part 4) which may then be the object of targeted requests (Part 3).

The DRIPA power

6.23. The DRIPA power allows for targeted access to similar records to those obtained by means of bulk acquisition. But those records are held by individual CSPs. We were told that a major advantage offered to the SIAs by bulk acquisition is the fact that data from a number of sources is aggregated.

6.24. That comment appeared to be confirmed by internal MI5 documents:

(a) The author of one such document noted that complex analysis on the aggregated system would be considerably more complex, and would take far longer.

(b) A further document recorded that *"one of the most valuable assets of [MI5's bulk acquisition capability] is the speed with which it is possible to retrieve [information] when necessary for the progress of an investigation."*

The speed advantage can be very significant in practice. For some operations (the London and Glasgow attacks being a strong example: A9/10) it is vital.

6.25. An additional advantage of aggregation accrues to GCHQ, which aggregates bulk acquisition and interception data.

6.26. I was curious as to whether the disadvantages of querying multiple databases (extra time, and greater difficulty in undertaking complex analysis) could be removed by the use of the filtering arrangements provided for in clauses 63-65 of the Bill. Those arrangements are promoted by the Government as "*an additional safeguard .. to prevent data from being provided to public authorities that is not relevant to the request*".[222] But when a parliamentary committee looked at the idea of a request filter in 2012, it concluded that as well as minimising collateral intrusion, "*the request filter will speed up complex enquiries*".[223] NGOs and others have sought to portray the arrangements as akin to merging separate databases into one.[224] If filtering arrangements ever become capable of emulating a single database, it could be argued that the comparative advantage of aggregating the data in one place would disappear.

6.27. I pursued this point with the Home Office officials entrusted with developing the filtering arrangements, who told me that they were still at the stage of defining requirements before going to the design phase. Its scope was uncertain, and there would be practical difficulties in bridging different formats. A prototype would have to be engineered, and a pilot phase operated. It was clear that a request filter will not be fully operational in the short term. Even when operational, it seemed doubtful whether it could fully emulate the characteristics of a single database.

6.28. For the time being at least, there are thus no filtering arrangements that could present an adequate alternative to the bulk acquisition power. But the matter needs to be kept under consideration. I return to this theme in chapter 9 below.

Other techniques

6.29. Within some of the case studies, MI5 itself identified potential alternatives. In many instances, those alternatives would have been more intrusive than the use of bulk acquisition, and that higher level of intrusion would have affected not only targeted individuals but entirely innocent members of the public. A9/14, a case in which MI5 needed to monitor terrorists who met in a place used by other people, provides a striking example: one alternative to bulk acquisition would have involved increased surveillance of members of the group. A further alternative of monitoring the meeting place would have involved an unacceptable level of intrusion into the lives of people completely unconnected to the targets.

---

222 Factsheet – request filter (published alongside the draft Bill in November 2015).

223 Joint Committee on the draft Communications Data Bill, Report of December 2012, HL Paper 79 HC 479, para 126.

224 E.g. K. Fiveash, "UK Govt sneaks citizen database aka 'request filters' into proposed internet super-spy law", The Register, 4 November 2015: an interpretation strongly contested by the Government.

6.30. The case studies also indicate that bulk acquisition may provide a more accurate result than targeted techniques, for example when the SIAs need to identify one phone among many candidates. Targeting each phone not only involves intrusion into the lives of phone users, many of whom will be of no intelligence interest at all, but also carries a greater risk that the right phone will not be identified at all. Although few details can be given in public, A9/15 illustrates this point.

6.31. The SIAs told the Review team that targeted alternatives (to bulk acquisition and other bulk powers) would often be more time-consuming and costly. A9/6 provides an example. We pressed for more details, and MI5 provided the following response:

> "Where alternatives to bulk capabilities exist, it is difficult if not impossible to say precisely how much additional resource, cost and time would have been required to obtain similar intelligence. At any one time, MI5 is likely to be running several hundred ICT [international counter-terrorism] investigations. MI5 (and SIS, GCHQ and the police) constantly prioritise resource across the breadth of our casework. The alternative combination of resources available (collection capabilities, numbers of investigators and analysts) and the speed in which they might have generated similar intelligence therefore depends not only on the specifics of the case, but also the wider threat picture and associated balance of resource being used to manage the risk at any one time."

6.32. While I cannot reach any firm conclusions about the level of cost or amount of time involved in the use of alternatives, it is obvious that some alternatives – such as round-the-clock surveillance, or a request to CSPs for data relating to dozens of phones, followed by analysis of that data – will cost more than a search being conducted in a matter of hours by a single analyst of bulk acquisition data. They may also be more intrusive.

6.33. Liberty submitted to the Review that the examples in the open Operational Case do not justify the use of bulk acquisition. It claims that the same results could have been obtained in some of the cases through the use of targeted techniques, in particular contact chaining, and that other examples provide insufficient detail for analysis.

6.34. On the latter point (only), I agree. The Review team had the substantial advantage of being given far more details of these cases than were made available in the Operational Case. But it was apparent to me that, in these cases, targeted means would not have been adequate alternatives. In some, MI5 did not have sufficient information to form the basis of a targeted approach. In others, a targeted request would not have provided the crucial information, or would have been too slow to be effective.

6.35. Many of the alternative techniques suggested by Liberty in more general terms would be far slower and less efficient than the use of bulk powers. Liberty argues, for example, that bulk powers are not needed to discover new methods of communication being used by a suspect. It contends that, instead, the SIAs could interrogate the target's bank records for evidence that the target has purchased a new device which they might then be able to identify and track. While such an approach might be possible, it would clearly take far longer than would be required to achieve the same result by a search of data acquired by bulk acquisition (or bulk interception). Further, as Liberty recognises, a search of banking records may not lead the SIAs to identify a new phone.

6.36. Liberty suggests targeted EI as a further alternative. Again, this may be a viable alternative in some situations, but not when the SIAs cannot identify the phone or computer being used by the target. EI of this sort may also be substantially more intrusive than the use of bulk powers.

Negative incidents and outcomes

6.37. There is no requirement under TA 1984 s94 to report an error when acquiring or accessing bulk communications data. MI5 has an internal policy process for reporting errors which cause communications data to be accessed wrongly. 230 such errors were reported to IOCCO in the 18 months from 1 January 2015, the great majority of them relating to a failure on the part of MI5 to follow their own handling arrangements and internal policies. After investigation, IOCCO concluded that the communications data accessed in those instances was nonetheless accessed for legitimate purposes, and found no evidence that the requirements of necessity and proportionality were not met.[225]

6.38. GCHQ has a mechanism for reporting errors to the IOCC, but cannot easily differentiate the source of the data as interception or s94 without compounding any potential intrusion, e.g. by re-running the erroneous query. It reported no errors to the IOCC that relate specifically to data obtained under a s94 direction. The IOCC has recommended that there be a clear mandated process in place for the reporting of errors.[226]

Internal documents

6.39. The majority of documents relating to bulk acquisition were supplied by MI5. It provided the Review team with copies of letters to the Home Secretary seeking renewal of its bulk acquisition authorisation, and with a variety of internal documents created for management purposes.

---

225 Report of the IOCC, July 2016, 8.79.

226 *Ibid.*, 8.84-8.84.

6.40. A letter to the Home Office from 2014 noted the value of the bulk acquisition power and expressed the view that "*[i]t would be difficult, if not impossible, to mitigate fully for the loss of these capabilities, as to do so would incur additional expense, resource and intrusion (direct or collateral) which may not be deemed proportionate under alternative mechanisms*".

6.41. A letter to the Home Office from 2015 described the bulk acquisition capability as "*one of the single most important capabilities available to MI5*" and stated that MI5 could not afford for there to be any break in the continuity of the service provided by the system.

6.42. A working level discussion document from 2016 noted that "*operationally, targeted CD powers cannot deliver the depth of intelligence, nor deliver at the same pace as Bulk CD*".

6.43. A GCHQ strategy paper for 2016-19 set out GCHQ's plans for the development and enhancement of its bulk data capabilities. It appears from that document that bulk acquisition was seen as having significant value to GCHQ, particularly in conjunction with data from other sources.

Conclusion

6.44. It was not open to me to disclose in AQOT the existence of the bulk acquisition capability that was exercised pursuant to directions under TA 1984 s94. Its avowal, on the morning that the draft Bill was presented to Parliament, was the first step to allowing its utility to be publicly evaluated.

6.45. I would have preferred to be able to give more detail in this Report as to the categories of CSPs and communications data that are currently subject to directions, the purposes for which applications for access are made and the uses to which the resulting data are put. Nonetheless, I have seen enough information to evaluate for myself the utility of the bulk acquisition power. I also note the conclusions of the IsComm and IOCC regarding utility: 3.87(b) above.

6.46. The SIAs assert that bulk acquisition offers the advantages over other techniques of speed and the ability to conduct more complex and comprehensive analysis. The case studies that I examined confirm the accuracy of that claim, particularly in respect of UK-based operations. Bulk acquisition is of more limited use when the help of overseas CSPs would be required to obtain the data. The SIAs' claim is also consistent with the terms of the internal documents that I have seen: it is clear that the SIAs regard bulk acquisition as vital to their activities.

6.47. I have concluded that:

(a) Bulk acquisition has been demonstrated to be crucial in a variety of fields, including counter-terrorism, counter-espionage and counter-proliferation. The case studies provide examples in which bulk acquisition has contributed significantly to the disruption of terrorist operations and, though that disruption, almost certainly the saving of lives.

(b) Bulk acquisition is valuable as a basis for action in the face of imminent threat,[227] though its principal utility lies in swift target identification and development.

(c) The SIAs' ability to interrogate the aggregated data obtained through bulk acquisition cannot, at least with currently available technology, be matched through the use of data obtained by targeted means.

(d) Even where alternatives might be available, they are frequently more intrusive than the use of bulk acquisition.

6.48. Those conclusions are consistent with the (albeit limited) opinions expressed or implied by the IOCC and the IsComm (3.12-3.13 and 3.21 above).

6.49. Once again, it should not be assumed that these conclusions will be the same for the foreseeable future. If (for example) filtering arrangements were to be developed which allows multiple databases effectively to be interrogated in the same way as a single database (6.26-6.28 above), the equation could change.

[227] See A9/25 (Northern Ireland dissident republican threat).

7. ASSESSMENT: BULK EQUIPMENT INTERFERENCE

Claimed utility

7.1. Bulk EI is unique among the powers under review in that it has not yet been used. The entire debate about its utility is thus focused on the SIAs' assessment of future developments in technology, on extrapolation from the use made of other powers, and on hypothetical case studies.

7.2. The Operational Case (8.1-8.2) locates EI, including bulk EI, in the context of diminishing returns from interception owing to technical developments such as end-to-end encryption[228] and the increasing anonymisation of network devices, making it harder to distinguish between target and non-target devices without at least some initial analysis of the data held on them:

> "Terrorists, serious criminals and hostile states have embraced technological advancements, including the widespread use of encryption, and the growth of the internet to hide from sight and to plan their attacks. As a result of this, the security and intelligence agencies can no longer rely solely on interception and are faced with an increasingly partial and fragmented intelligence picture, even when investigating known threats. If the security and intelligence agencies are to be able to maintain the same understanding of threats and be able to disrupt them, they need to use other, and complementary, techniques which will provide comparable pieces of the intelligence jigsaw.
>
> Bulk EI describes a set of techniques to obtain information from devices that is necessary for the identification of subjects of interest who pose a threat to the UK's national security, in circumstances where the information is not available through the use of other methods. Bulk EI enables the security and intelligence agencies to overcome techniques used by subjects of interest to hide their identities or their communications."

7.3. Bulk EI is distinguished from targeted thematic EI not on the basis of its scope (since both may take place "*at scale*", covering "*a large geographical area*" or involving "*the collection of a large volume of data*") but on the basis that there will be cases in which

> "the Secretary of State and the Judicial Commissioner is not .. able to assess the necessity and proportionality to a sufficient degree at the time of issuing the warrant",

[228] Google announced in February 2016 that 77% of requests received by Google servers from computers around the world were encrypted, up from 52% in 2013. MI5 told us that the majority of the top 40 online activities relevant to their intelligence operations are now encrypted.

for example "*where the purpose of the operation is target discovery and the security and intelligence agencies do not know in advance the identity of the new subjects of interest who threaten the security of the UK and its citizens*".[229]

7.4. All the SIAs saw EI as of growing importance across the full range of threats to the UK, driven by the increasing use of encryption and diversity of communications methods. GCHQ described CNE (the principal component of EI) as enabling the state "*to obtain the valuable intelligence it needs to protect its citizens from individuals involved in terrorist attack planning, kidnapping, espionage or serious organised crime*" (Annex 7). GCHQ managers stated that they did not expect bulk EI to form a large part of GCHQ's work but thought that it would underpin other work, and would be used in the first instance before targeting was possible.

7.5. MI6 considered that it was likely to become "*increasingly dependent*" on GCHQ's use of bulk EI to identify threats to the UK, to develop its understanding of those threats and to disrupt them, particularly in the context of counter-terrorism and cyber (Annex 6).

7.6. It was emphasised that bulk EI operations will be designed to bring back the minimum amount of information required to rule out devices not of intelligence interest. That would often imply a "*light touch*" operation targeted at least in the first instance on equipment data (the EI equivalent of secondary data). This would allow more targeted approaches to be made.

7.7. I was told however that the power to obtain content was also likely to be useful in certain circumstances:[230]

(a) It was possible that the "*seed*" information which GCHQ has about targets could relate to information defined as content under the Bill: for example, a particular video or the use of a particular combination of elements. If the spread of encryption means that bulk interception cannot be used for this purpose, bulk EI may have to take its place.

(b) Once an initial engagement or series of engagements had identified devices of interest, malware could be written or implants designed so as to obtain content from those devices.

---

229 Operational Case, March 2016, 8.5-8.7. An illustration of the different situations in which targeted thematic EI and bulk EI would be required was set out at 8.8 of the Operational Case, and is reproduced at A10/6.

230 Clause 162(1)(b)(i),

Scale of use

7.8. The Review team was told that about 50% of Internet traffic was now encrypted, and 100% of emails from major email providers. It was not possible, nor would it be desirable, for GCHQ to decrypt all such traffic, so alternative methods of obtaining information had to be sought.

7.9. Thematic EI is currently used by GCHQ and to a lesser extent by MI5 and MI6.[231] Bulk EI is not currently used at all: though the Bill allows all SIAs to use it, it is envisaged that, like bulk interception, it will be practised only by GCHQ.

7.10. Currently around one in five GCHQ intelligence reports is based on material obtained from targeted EI.[232] Data obtained from targeted EI provided roughly a fifth of GCHQ's intelligence, and more than a third of higher grade intelligence.

Case studies (Annex 10)

7.11. The case studies relating to bulk EI are set out at Annex 10, but are necessarily very limited in view of the fact that GCHQ has not yet used the power.

7.12. The Review team was introduced to two real-life case studies (A10/1-2) in which an EI warrant was obtained under ISA 1994, in circumstances in which, were the Bill in force, a thematic targeted warrant would be sought. Both involved the identification of extremists in Syria who could pose a threat to the UK, or to UK nationals – as potential hostages – in Syria. Both involved target identification and subsequent development, and both involved only the obtaining of systems data.

7.13. The Review team saw internal GCHQ material in which further explanations were given of situations in which content might be obtained through bulk EI.

7.14. I also considered the hypothetical examples of the use of bulk EI set out in the Operational Case, concerning respectively counter-terrorism, counter-proliferation, cyber-defence and the difference between thematic and bulk EI (A10/3-6). They do not have the value of real examples, but help to explain the type of future operation in which GCHQ might plausibly propose to use bulk EI.

---

231 Police forces are also to be given the power, if duly authorised, to use targeted EI (including targeted thematic EI) under Part 5 of the Bill: clauses 100, 101.

232 As recorded in *Privacy International v The Secretary of State for Foreign and Commonwealth Affairs* [2016] UKIPTrib 14_85-CH, para 5(ii).

Alternative methods

Interception

7.15. Interception was not a viable alternative in either of the thematic EI case studies (A10/1-2). Nor of course was it viable in the hypothetical examples that were written with that scenario in mind (A10/3-5), or in the case study written to illustrate the difference between thematic and bulk EI (A10/6).

7.16. Interception may not be an adequate alternative because of technological developments such as the anonymisation of devices and end-to-end encryption, but also because the physical location of targets makes interception impossible, or indeed because the target is not communicating. EI can be used to obtain data on a device without that data ever having been sent anywhere by the user.

Targeted EI

7.17. The four reasons why a targeted interception warrant may not be a feasible alternative to a bulk interception warrant (5.24 above) do not apply (or do not apply in the same way) in the EI context. Rather, the case for the inadequacy of targeted EI as a substitute for bulk EI is put on the basis of the trend towards the anonymisation of devices. This is said to mean that in future, GCHQ will increasingly need to conduct operations in which it is not fully possible to assess the degree of intrusion, at the point of authorisation and approval, because it does not at that point have sufficient information about the equipment with which it will interfere, the data it will collect or the precise analysis that will be required. This would rule out even thematic EI, which should be used only when it is possible to foresee the extent of the intrusion of the outset.

7.18. Thematic targeted EI may be of equivalent scope to bulk EI, and a warrant should therefore be no more cumbersome to obtain. But it is hard to see thematic targeted EI as less intrusive alternative to bulk EI. Indeed there are fewer limitations on its use, as described at 2.52-2.58 above.

Human sources

7.19. In A10/1-2, GCHQ identified human sources as the only (albeit theoretical) alternative means of obtaining information. In practical terms, the operating environment was too dangerous for the use of human agents. It would also have taken far longer for agents to obtain the information than it took analysts using EI. It also appears likely that EI provided a more complete picture than agents would have been able to achieve.

No alternatives

7.20. A substantial part of bulk EI's value lies in the very fact that its use is envisaged when no alternatives are available. It is clear from GCHQ's internal documents (discussed below) that it sees EI, including at scale, as a capability crucial to its future operations. It is being developed because (at least in part) interception has been rendered less effective by the use of encryption.

7.21. Liberty in its submission to the Review contends that the first and second hypothetical examples in the Operational Case (A10/3-4) do not demonstrate that the "*population level*" use of bulk EI powers overseas would have been either necessary or proportionate. It argues that the third hypothetical example (A10/5) provides insufficient detail for useful analysis.

7.22. I accept that there is an artificiality in reliance upon hypothetical examples, and that in any given situation there will be questions as to whether less intrusive and equally effective methods could not have been used. But having discussed these examples, and examined in some detail case studies in which the thematic EI power was used, I conclude that there could in the future be situations in which the availability of a bulk EI power will bring useful results not achievable by other means.

Negative incidents and outcomes

7.23. The IsComm's first open report on EI will be published only in September 2016, as noted at 3.20 above, and may be expected to record reported errors (as did its confidential predecessors).

7.24. As noted at 1.39 above, we always suspected that teething trouble and wrong turns were likely to be experienced with new EI techniques. GCHQ disclosed to the Review team an internal document which referred to "*shortcomings*" and a lack of success in CNE techniques in one particular aspect of GCHQ's work. GCHQ provided an explanation of this reference. I was told that the use of CNE had not been a success in this field because resources had been diverted from that area of work; the same technology might well have been working successfully in another field to which more time and money were devoted. GCHQ managers accepted that the technology was new, and that, in certain operations, the technology would require development in order to achieve the desired result.

7.25. The Review team was provided with examples of a number of incidents in which CNE work had caused unintended consequences to targeted computers. In most of these examples, a computer failure obvious to the user had occurred (although the user would probably not have been aware of the cause). In one

case, the *"impact*" was believed to be imperceptible to the user. The documents indicated that there had, in recent years, been an increase in the number of "*unexpected incidents*", although the most recent figures showed a reduction. The increase was attributed to the increase in CNE work and to greater investigation by GCHQ of incidents involving CNE.

7.26. Serious allegations have been made about the potential of CNE to create security vulnerabilities or leave users vulnerable to damage: 2.68(b) above. It is not for me to determine the truth of such allegations. But it is plain from everything I have seen that, notwithstanding the technical shortcomings referred to above, EI, including at scale, is capable of producing useful results.

Internal documents

7.27. The Review team was given access to a substantial number of quarterly and annual GCHQ reports, including GCHQ Investment Board minutes and papers submitted to the Board. In addition, we were shown strategy and business case documents relating to GCHQ's present activities and future plans.

7.28. The difficulties caused to GCHQ's work in many fields by increasing encryption, and the need to develop greater CNE capabilities, were recurring (and linked) themes throughout the reports.

7.29. Business case documents from 2012 to 2016 have consistently advocated the need for the further development of EI, including by "*CNE scaling*". A series of documents dating from 2013 and 2014 set out the need for change in the light of technological advances, and stated that CNE would be expected to play a greater part, relative to bulk interception, than had previously been the case. Two papers from 2014 referred to the aim of "*shift[ing] GCHQ from a predominantly passive access organisation to one where active and passive approaches are in balance and mutually reinforcing*".[233] The desirability was stressed of attaining a clear legal basis for "*bulk CNE*", described as "*the delivery of implants to devices not precisely identified in advance, for the purpose of discovering targets*".

7.30. The annual mission report for the 2015-16 financial year recorded significant success in GCHQ/MI5 operations designed to protect major private businesses (including those providing essential services such as energy, telecommunications, transport and water) from cyber-attack. CNE was described in the mission report as being "*fundamental*" to GCHQ's work to combat cyber-

[233] Passive access refers to the ability to reach traffic because it flows past an interception point, generally without the need to actively interfere with the communications or with any user devices. An active approach interferes with the traffic or with a user device, in particular by CNE / EI.

crime, and to addressing the difficulties caused in this field by the increasing use of encryption.

7.31. The author of the GCHQ 2015-16 end of year performance report, addressing GCHQ's coverage of the Islamist threat outside the UK, noted that the use of CNE had led to the production of "*uniquely valuable intelligence*" in respect of the threat.

Conclusion

7.32. The bulk EI power is unlike all the others, in that (though the dividing line between bulk and thematic is not always very clear) it has never been used.

7.33. It is plain however that, as the internal documents abundantly demonstrate, EI is a fast-developing alternative to bulk interception (albeit one that in GCHQ's own jargon is described as "*active*" rather than "*passive*".

7.34. I also accept that the logic of bulk interception transposes to EI, in that there will be foreign-focused cases in which there is significant value to be gained for GCHQ's operational purposes but in which it will not be possible to make a sufficiently precise assessment to proceed on the basis of the thematic EI power. I would also repeat, as noted at 2.52-2.58 above, that the additional constraints attaching to the use of bulk EI render it in some respects a more palatable tool than the thematic EI power.

7.35. A10/1-2 are both examples of targeted thematic EI in respect of which the only possible alternative, the use of human sources, was unrealistic. It was possible to envisage situations fairly similar to those of the case studies in which insufficient information was available to justify a warrant for targeted thematic EI. The three hypothetical examples in the open Operational Case (A10/3-5) are also plausible indications of scenarios in which bulk EI could be needed.

7.36. For all these reasons, I conclude (as, after full consideration, did the Chair of the ISC: 3.87(c) above) that an operational case for bulk EI has been made out in principle, and that there are likely to be real-world instances in which no effective alternative is available. While it is likely to be of use in particular for the recovery of equipment data, its capacity to recover content may also be of value (7.7 above).

7.37. But very considerable caution is required, in view of:

(a) the fact that EI can recover data that has never been sent anywhere (7.16 above);

(b) the untried nature of the power;

(c) the fast-evolving range of offensive techniques that can be applied, and the likely speed of future technical developments; and

(d) the capacity of EI, particularly when used at scale, to cause, even inadvertently) lasting harm to networks and to devices (2.68(b) and 7.24-7.25 above.

7.38. All this means that bulk EI will require, to an even greater extent than the other powers subject to review, the most rigorous scrutiny not only by the Secretary of State but by the Judicial Commissioners who must approve its use and by the IPC which will have oversight of its consequences.

8. ASSESSMENT: BULK PERSONAL DATASETS

Claimed utility

8.1. All three SIAs retain and use BPDs, though GCHQ uses them to a lesser extent than MI6 and MI5. The Operational Case describes BPDs as "*an essential tool*" for the SIAs, without which "*the security and intelligence agencies would be significantly less effective in protecting the UK against threats such as terrorism, cyber threats or espionage*".

8.2. The case for the utility of BPDs is spelled out in the Operational Case as follows:

> "BPD enables the security and intelligence agencies to focus their efforts on individuals who threaten our national security or may be of other intelligence interest, by helping to identify such individuals without using more intrusive investigative techniques. It helps to establish links between subjects of interest or better understand a subject of interest's behaviour. BPD also assists with the verification of information obtained through other sources (for example agents) during the course of an investigation or intelligence operation.
> …
> Using BPD also enables the security and intelligence agencies to use their resources more proportionately because it helps them exclude potential suspects from more intrusive investigations."[234]

8.3. MI5 told the Review that it used BPD "*to quickly develop fragmentary intelligence into a real world identity*", to understand adversaries and the links between them, and to inform disruptive action. It emphasised the importance of BPD (and bulk acquisition) for ruling out individuals whose privacy might otherwise have been intruded into (a point also made in this context by GCHQ: Annex 7), commenting that "*without bulk capabilities, MI5 simply could not effectively process and respond to the volumes of incoming leads*" (Annex 5).

8.4. For MI6, BPDs "*often form the backbone of investigative work*" (Annex 6). In particular, BPDs:

(a) enable MI6 to "*take a piece of fragmentary information and make a positive identification of a person of intelligence interest who could not otherwise be identified*", and

(b) "*help [MI6] to better understand the risks surrounding its activities in order to protect the people it works with all over the world*".

It described BPDs as "*equally important across all operational areas covered by [MI6] including counter-terrorism, counter-proliferation, cyber, serious crime and*

234 Operational Case, March 2016, 10.4 and 10.6.

the geographical requirements for intelligence collection set out in the National Security Strategy", and considered that their importance to MI6 was likely to increase.[235]

8.5. GCHQ told the ISC that it considered BPDs to be an increasingly important investigative tool, which it used primarily to "*enrich*" information that it had obtained through other means.[236]

8.6. I was briefed by Lynne Owens, Director General of the NCA, in relation to a specific respect in which a hypothesis regarding the behaviour of persons involved in child sexual exploitation was tested and rebutted by the use of intelligence from bilk data retained and used by the SIAs (cf. A8/10). That intelligence resulted in a marked and productive change in the way that crime of that kind is investigated. More generally, the NCA characterised bulk data as offering "*a different and unique intelligence picture, not obtainable through other means*".

Scale of use

8.7. The Government claims that BPDs are used by the SIAs "*on a daily basis, in combination with other capabilities, right across the security and intelligence agencies' operations*".[237]

8.8. I was told that:

(a) All investigative staff and analysts at MI5 have access to BPDs (though some of the datasets are restricted to analysts only).

(b) Around 80% of people working on intelligence operations in MI6 have access to BPDs.

(c) Around 10% of those working on intelligence operations at GCHQ have access to BPDs.

8.9. The IsComm reports on the procedures by which BPDs are selected for use by the SIAs (3.18 above), but has not quantified the use made of BPDs by the SIAs.

Case studies (Annex 11)

8.10. MI6 provided the Review team with 24 case studies in the form of brief summaries. The open version of one of these studies had already been made public as part of the Operational Case. A further five had been provided privately

235 GCHQ considered that the importance of BPDs to its operations would remain the same: Annex 7.

236 2015 ISC Report, para 153.

237 *Ibid.*, 10.3.

to the Intelligence and Security Committee on 29 February 2016. At the Review team's meeting with MI6, the team was given further details of seven of the MI6 case studies. Cathryn McGahey QC returned for a second visit to examine contemporaneous documents relating to those case studies, and to be given a demonstration of analysis using BPDs. I had been given a similar demonstration when preparing *A Question of Trust.*

8.11. MI5 gave the Review team a further ten summaries, six of which had featured in the Operational Case.

8.12. Annex 11 summarises the seven MI6 case studies that the Review team examined in detail, and a sample of the ten MI5 cases.

8.13. The case studies demonstrated the use of BPDs as a swift and efficient method of identifying potential MI6 agents (A11/1,4), hostile state actors (A11/2-3), and potential terrorists (A11/5-15). Some demonstrated clearly the utility of BPDs in reducing a very large pool of potential candidates to a manageable number. For example, in A11/8, MI5 was able to identify an individual from a pool of some 27,000, and to take steps to disrupt that person's extremist activities.

8.14. BPDs have been used both to identify individuals of interest and to eliminate from an investigation those who are not of interest. A11/11 involved the use of BPDs both to identify some persons suspected of posing a potential threat to the London Olympics and to exclude others from suspicion. BPDs enabled MI5 swiftly to identify, from among a large number of individuals working for the Olympics, those who should be prioritised for investigation. There was a clear need for such work to be carried out at speed.

Alternative methods

8.15. MI6, a principal user of BPDs, does not assert that it could not carry out its work without them. Managers explained to the Review team that MI6 has recruited agents for many years, and would always find ways to do so. However, managers firmly believed that, without BPDs, MI6's work would be less efficient, and carry greater risk, and that opportunities would be missed. The pace at which the SIAs were now required to work, particularly in the field of counter-terrorism, was substantially greater than it had been in the past.

8.16. When seeking to recruit an agent, with only partial information about his identity, the use of BPDs may enable MI6 to identify the relevant person speedily, economically and safely. The obvious alternative, of sending an existing agent to confirm an identity, may take weeks and put that agent at risk. Such a course is also far more resource-intensive than the use of BPDs.

8.17. MI6 made a similar point to the Review team about the effectiveness of BPDs in respect of target development. Much may be learned about a person through the interrogation of BPDs. The alternative to the use of BPDs may be the interception of that individual's communications, a far more intrusive method.

8.18. Alternatives are frequently much slower. A11/6 involved the use of BPDs to confirm the partial identities provided on 20,000 ISIL registration documents. Identification using alternative means would inevitably have been a far more laborious process, and might well not have provided as many confirmed identities.

8.19. BPDs are also used in the identification of anomalies: analysis of BPDs may lead to the identification of patterns which reveal hostile activity. In this field, BPDs enable an agency to spot such activity without even having the "seed" of intelligence which is usually required to start such an investigation. In the absence of such a seed, there is no alternative means to obtain the intelligence. The identification of anomalies may lead to the discovery of hostile actors who would not otherwise have come to the attention of the SIAs or police. A11/2 provides an example of pattern analysis leading to identification that would not otherwise have occurred.

8.20. A11/5 demonstrates the use of BPDs this year, by MI6 in partnership with MI5 and GCHQ, to identify individuals who posed a threat to the UK in the wake of the Paris and Brussels attacks. The Review team was given information which demonstrated that there was no viable alternative method by which these individuals could have been identified.

8.21. In its submission to the Review of 31 July 2016, Liberty suggests that the acquisition of BPDs by the SIAs is a "*new and radical development*" (inaccurately: 2.70 above), and claims that the SIAs can obtain through other means the information that they need in respect of specific targets.

8.22. Liberty argues, in particular, that even a "*lone wolf*" must be radicalised, obtain weapons and come into contact with extremist material. It appears to be contending that targeted surveillance of those with whom a lone operator comes into contact will lead to his identification. That may be true in specific instances, but depends entirely on the SIAs having knowledge of, and the resources to monitor, those potential contacts.

8.23. Liberty states that it is "*highly likely*" that an SIA in possession of a target identifier will be able to identify the target by name, and will then be able to deploy a range of targeted techniques against him. There will undoubtedly be circumstances in which the SIAs may use targeted techniques against an identifier and thereby discover the target's name. But the Review team was

shown case studies from which it was apparent that the use of bulk powers (notably BPDs, but also communications data obtained by bulk interception and bulk acquisition) was particularly valuable in enabling SIAs to identify an individual from a partial identifier: A8/3,10; A9/1; A11/6,8-10.

8.24. In its critique of the Operational Case, Liberty makes the entirely valid point that some of the case studies provide insufficient detail for any useful analysis to be conducted or conclusions drawn. But having questioned SIA staff and examined the underlying documents, including intelligence reports, my informed view is that the power is of real utility. It is right to say that in some instances alternatives would be available, but they all had disadvantages, often of slowness, cost, greater intrusiveness or risk to human agents.

Negative incidents and outcomes

8.25. The IPT was told in March 2016 that between 1 June 2014 and 9 February 2016, six instances of non-compliance with handling requirements were detected at MI5. In three of those cases, a dataset was mistakenly left out of MI5's BPD review process, so that the necessity and proportionality of retention was not reconsidered for between one and two years. In one further case, a dataset which fell within the definition of a BPD had not been entered into the BPD process. The final two instances were of individual acts of non-compliance by staff members. Two members of staff had been disciplined.

8.26. During the same period, five instances of non-compliance were detected at MI6. Two involved BPDs being ingested into the system before they had been authorised. In both cases, BPDs were removed as soon as the error (caused by ambiguity within MI6's IT systems) was detected. The remaining three errors involved individual non-compliance. Three members of staff were disciplined.

8.27. Two instances of non-compliance were detected at GCHQ during this time. In the first, the retention of a dataset acquired and approved in 2012 was not subsequently re-authorised. The second instance involved a BPD that was first acquired in 2010 but not recognised as a BPD until 2015.[238]

8.28. More broadly, there is no measurement of "*failed searches*" of BPD. But in each SIA, there is ongoing review of BPDs that are held in order to determine whether they are as valuable to operations as was envisaged when they were first acquired. At retention reviews, some BPDs are deleted if their contribution to operations has declined. This review of the relative value of BPDs informs decision-making about future acquisition.

---

238 *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others, Case No. IPT/15/110/CH,* redacted Closed Response of the Respondents to the Claimants' Request for Further Information and Disclosure, 30 March 2016.

Internal documents

8.29. There is abundant internal documentation evidencing the value of BPDs to the SIAs.

8.30. I was shown MI6 business proposals dating from 2005 to 2011 in respect of the development of BPDs. The earliest documents set out the need for such datasets and the budget required for them; subsequent documents track the development of BPD systems and the need for funds to be spent on upgrading them. In 2011 the BPD system was described as "*a mission critical tool which is highly valued by the Service and is making an important contribution to the work of operational teams*". The same document described BPDs being used to produce new intelligence, develop knowledge of current operations, carry out agent recruitment, tasking and evaluation and identify operational threats. It was claimed that BPDs "*were considered to have the potential to save lives*", and described them as "*a vital tool to operational officers, who are demanding more from the system than was planned*".

8.31. MI5 documents are extremely supportive of the value of BPDs. For example:

(a) In an internal document of July 2014, the Deputy Director General wrote: "*It is clear that access to BPD is now critical to our core investigative, operational and analytical businesses ... its value is beyond doubt.*"

(b) A bulk data strategy document from 2014 stated that BPDs were "*an essential part*" of MI5's work to address gaps in its coverage, a conclusion repeated in a paper setting out MI5's 2015-16 strategy for its Northern Ireland operations.

(c) A strategy paper of June 2015, addressing the use of BPDs in counter-terrorism operations, noted:

> "Although BPD provides little or no insight into the mind-set or intent of an individual, its key advantage is the breadth of coverage. Our ability to fuse multiple expansive data sets for analysis offers unprecedented opportunities to resolve complete identities of individuals based on partial details ... As such BPD is fundamental to CT investigations ...".

(d) An internal paper dated July 2015, written for MI5's Executive Board, stated that "*we derive significant value from our bulk data holdings*" and that "*The rapid development of new technologies and data types (e.g. increased automation, machine learning, predictive analytics) hold additional promise ...".*

(e) A set of slides used to present BPD strategy in September 2015 set out a number of uses to which BPDs were put: to resolve the identities of subjects of interest **[SOIs]** and establish their whereabouts; to identify activity of interest; to provide assurance on defined investigative questions; to identify SOI access of interest (e.g. to establish whether a target was working in a particular sector); to establish disruption opportunities; to establish investigative opportunities; to identify contacts of SOIs and to identify and protect targets of SOIs.

(f) An internal paper of June 2016, setting out the strategy to 2018 for a department within MI5, pointed to the use of BPDs in providing "*building-block*" intelligence that would progress investigations in an efficient and focused way; targeting the activities of foreign actors; providing ongoing verification of agent reporting; and enabling defensive capabilities to protect UK Government information from unauthorised disclosure by others.

8.32. The Review team has also had the opportunity to inspect the "*retention forms*" that are completed at each of the Agencies when their staff seek authorisation to retain a particular BPD. Each form sets out the perceived usefulness of the BPD in question and the frequency with which it is used, provides an assessment of its value and also (in the case of MI5 and GCHQ, though not MI6) gives specific examples of operations in which the BPD was used.

Conclusion

8.33. I have no hesitation in concluding that BPDs are of great utility to the SIAs. The case studies that I examined provided unequivocal evidence of their value. Their principal utility lies in the identification and development of targets, although the use of BPDs may also enable swift action to be taken to counter a threat.

8.34. BPDs are already used elsewhere, in the private as well as the public sector, with increasing sophistication. Their utility to the SIAs has been acknowledged by successive IsComms and by the ISC: 3.87(d) above. As I concluded in AQOT 8.106: "*It may be legitimately be asked, if activity of a particular kind, is widespread in the private sector, why it should not also be permitted (subject to proper supervision) to public authorities*".[239]

8.35. BPDs are used by the SIAs for many purposes: for example, to identify potential terrorists and potential agents, to prevent imminent travel, and to enable the SIAs to prioritise work. It will often be possible, in a given instance, to identify an alternative technique that could have been used. However many such alternatives would be slower, less comprehensive or more intrusive. The value

[239] See, generally, AQOT 8.65-8.106 for a discussion of private sector use of personal data and its implications for the use of investigatory powers by the state.

of accurate information, obtained at speed, is considerable. I accept the claims of MI5 and MI6 that their work would be substantially less efficient without the use of BPDs and GCHQ's claim that it finds BPDs useful to enrich information obtained through other means.

8.36. In some areas, particularly pattern analysis and anomaly detection, no practicable alternative to the use of BPDs exists. These areas of work are vital, since they can provide information about a threat in the absence of any other intelligence seed. The case studies included a cogent example of the value of pattern analysis (A11/2).

8.37. The use to which bulk data can be put is in the course of rapid evolution. MI5 recognised in July 2015 that the development of new technologies and data types, including machine learning and predictive analytics, offered "*additional promise*" in this field. Future decision-makers authorising and approving the use of BPDs will have to be aware of these technological advances, and the effect that they have both on the availability of alternatives and on the extent of intrusion involved in the use of BPDs.

9. CONCLUSIONS AND RECOMMENDATION

Privacy and safety

9.1. The essential starting-point for any law on investigatory powers is "*the right to respect for .. private life, home and communications*" and "*the right to protection of personal data*".[240] These legal rights are sometimes expressed in terms of the right to be let alone, the right to conceal information about ourselves or the right to control our own affairs. They enable the expression of individuality, facilitate trust, friendship and intimacy, help secure other human rights and empower the individual against the state.[241]

9.2. Privacy is not simply an interest to which public authorities must have regard, but a right into which intrusions will be countenanced only on tightly specified conditions.[242] While the individual impact of a privacy intrusion may be imperceptible or trivial, as may repeated intrusions of a purely technical nature,[243] the cumulative effect of surveillance (and the fear of surveillance) on the way we perceive ourselves and relate to others can be very marked.[244]

9.3. But international human rights instruments are pragmatic enough to recognise that intrusions into individual privacy will often be justified in the public interest. The privacy right may be overridden, where it is proportionate to do so, in the interests of national security, safety and the prevention of disorder or crime.[245]

9.4. Just as much as privacy itself, each of those interests has a human dimension. They are essential if people are to enjoy a healthy individual, social and political life. As I have previously written:

---

240 These formulations, taken from the EU Charter of Fundamental Rights, Articles 7 and 8, are updated from "*the right to respect for private .. life .. home and correspondence*" in ECHR Article 8. See further AQOT 5.12-5,23 and 5.57-5.58. But such rights are universal, not just European: see International Covenant of Civil and Political Rights 1966, Article 17; AQOT 5.84-5.91.

241 See AQOT 2.4-2.13.

242 The protection afforded by the Human Rights Act 1998 (acknowledged in clause 1(4)(b) of the Bill) and by the ECHR thus extends beyond the "*general privacy protections*" in Part 1 of the Bill, e.g. the duty on public authorities to have regard to the public interest in the protection of privacy (clause 2(2)(c)).

243 It is difficult, for example, to see more than theoretical privacy intrusion in the techniques by which bulk powers are used to locate malware and prevent cyber-attacks.

244 AQOT 2.8, citing the comparison made with environmental damage by J. Angwin, *Dragnet Nation: A quest for privacy, security and freedom in a world of relentless surveillance*, 2014.

245 The legal significance of the familiar terms "*necessity*" and "*proportionality*" is not altogether straightforward: AQOT 5.18. I have accordingly (in keeping with my terms of reference) avoided pronouncing on whether the powers under review are "*necessary*", a word which in its everyday meaning could be taken to encompass assessments of proportionality or overall desirability which are excluded from my remit.

> "A person who lives in fear of anti-social behaviour, online harassment, neighbourhood drug gangs or persistent nuisance calls is patently unable to experience individual security or self-fulfilment.
>
> The trust in strangers on which civilised society depends is eroded by a perception that cyber fraud is prevalent, that rogue tradesmen prey on the old with impunity or that paedophiles flourish in the privacy of their homes.
>
> The threat of terrorist atrocities curtails normal activities, heightens suspicion, promotes prejudice and can (as the terrorist may intend) do incalculable damage to community relations.
>
> A perception that the authorities are powerless to act against external threats to the nation, or unable effectively to prosecute certain categories of crime (including low-level crime), can result in hopelessness, a sense of injustice and a feeling that the state has failed to perform its part of the bargain on which consensual government depends."[246]

9.5. Each of the case studies which the Review team has considered is said to represent a success, small or large, against serious crime or threats to national security. They all involve intrusions, however technical, into the rights set out at 9.1 above. But as they also illustrate, the benefits of successful operations are not simply measurable in a dry tally of operational gains. Individually and cumulatively, they change lives for the better.

The sensitivity of bulk powers

9.6. I have elsewhere described the question of whether the bulk collection and retention of data are compatible with international privacy protections as "*a human rights issue in relation to this Bill that dwarfs all others*".[247] That is because:

(a) Bulk powers, by definition, involve potential access by the state to the data of large numbers of people whom there is not the slightest reason to suspect of threatening national security or engaging in serious crime.

(b) Any abuse of those powers could thus have particularly wide-ranging effects on the innocent.

(c) Even the perception that abuse is possible, and that it could go undetected, can generate a corrosive mistrust.

---

246 AQOT 3.8. The reference to low-level crime, important though its effects may be, is not relevant to the powers under review. In recognition of their extensive nature, the Bill permits them to be exercised only when there is a national security purpose or (in the case of BPDs) to combat serious crime.

247 Oral evidence to the Joint Committee of Human Rights, HC 647, 9 March 2016, Q13.

9.7. None of those factors is a reason in itself for renouncing the use of bulk powers.[248] They do however mean that the use of bulk powers should only be countenanced if there is a ***compelling operational case*** for their use, and if their use is subject to ***adequate and visible safeguards***.

The function of this Report

9.8. It is not the function of this Report to pronounce on the overall case for bulk powers. The Government has been clear that "*consideration of the safeguards that apply to [the bulk] powers, and associated questions of proportionality*" should not form part of this Review, on the basis that these are "*rightly a matter for Parliament to consider as part of its scrutiny of the Bill.*"[249]

9.9. The task of the Review team has been more straightforward but also more technical: to "*examine the operational case for the investigatory powers contained in Parts 6 and 7 of the Investigatory Powers Bill*", and as part of that exercise to "*assess whether the same result could have been achieved through alternative investigative methods*".[250] The fact that an intrusive power can be successfully used to avert threats and reduce crime does not of course mean that it should automatically be passed into law: that way lies a police state. But as my terms of reference imply, a strong operational case is the essential starting point, without which the political debate is not worth having.

9.10. This is not virgin territory: as narrated in chapter 3 above, a variety of other security-cleared persons have looked carefully at related questions. It would be wrong to dismiss them as mere creatures of the establishment: among the strongest defenders of the utility of the powers have been successive Commissioners who bring to their task the dispassionate and forensic qualities of a senior judge, the additional independence that accompanies retirement and, in the case of IOCC, a substantial team of skilled inspectors. Like the better-known work of the PCLOB in the US, their reports (and future reports of the IPC, which will have access to further sources of expertise) deserve to be a primary point of reference for international rapporteurs and tribunals which themselves lack the same access to classified materials.

9.11. I have discussed my provisional conclusions with other members of the Review team, and sought to stress-test them by reference to the widest possible variety of sources (chapter 4 above). To a large extent, they conform to the views

---

248 That would certainly appear to be the position of the ECtHR (3.78-3.80), though the CJEU may be signalling a more absolutist position, at least where "*access on a generalised basis to the content of electronic communications*" is concerned: 2.28 above.

249 See 1.11 above. Parliament is well equipped to decide these issues, bearing in mind the seven reports that its own committees have already produced, as well as the three that preceded the introduction of the draft Bill: 1.16 and 1.22 above.

250 See 1.10 and 1.13, above.

expressed by others who have looked at these issues on a security-cleared basis. My conclusions, and my reasoning to the extent that I have been able to explain it, are now open for discussion and debate. I hope that they will help to inform what remains of the parliamentary consideration of the Bill.

The strength of the operational case

9.12. I have already summarised what I consider to be the strength of the operational case for each of the bulk powers (chapters 5-8 above). Among the other sources of evidence referred to in chapter 4 above, I have based my conclusions on the analysis of some 60 case studies, as well as on internal documents in which the SIAs offered frank and unvarnished assessments of the utility and limitations of the powers under review.

9.13. The sheer vivid range of the case studies – ranging from the identification of dangerous terrorists to the protection of children from sexual abuse, the defence of companies from cyber-attack and hostage rescues in Afghanistan – demonstrates the remarkable variety of SIA activity. Having observed practical demonstrations, questioned a large number of analysts and checked what they said against contemporaneous intelligence reports, neither I nor others on the Review team was left in any doubt as to the important part played by the existing bulk powers in identifying, understanding and averting threats of a national security and/or serious criminal nature, whether in Great Britain, Northern Ireland or further afield.

9.14. My specific conclusions, in short summary, are as follows:

(a) The ***bulk interception power*** is of vital utility across the range of GCHQ's operational areas, including counter-terrorism, cyber-defence, child sexual exploitation, organised crime and the support of military operations. The Review team was satisfied that it has played an important part in the prevention of bomb attacks, the rescuing of hostages and the thwarting of numerous cyber-attacks. Both the major processes described at 2.19 above produce valuable results. Communications data is used more frequently, but the collection and analysis of content has produced extremely high-value intelligence, sometimes in crucial situations. Just under 50% of GCHQ's intelligence reporting is based on data obtained under bulk interception warrants, rising to over 50% in the field of counter-terrorism.[251]

(b) The ***bulk acquisition power***, undisclosed until November 2015 and used by MI5 and GCHQ, has similarities with the DRIPA power but has two significant advantages: ability to perform complex analysis and greater speed of use.

[251] See chapter 5 above, in particular 5.8-5.10 and 5.50-5.55.

For MI5, it has contributed significantly to the disruption of terrorist operations and to the saving of lives. GCHQ gains benefit from merging the data with the product of bulk interception, and claims to use the power across the range of its operational work, though we saw only one case study to illustrate this. The power is useful in eliminating lines of enquiry and so focusing resources where they are needed. It is extensively used on a daily basis, and contributes material to some 5% of GCHQ's intelligence reporting.[252]

(c) The ***bulk EI power*** is not currently authorised and has never been used, though targeted EI is seen as an important capability across the full range of threats to the UK, driven by increasing use of encryption and diversity of communications methods. EI already contributes to some 20% of GCHQ's intelligence reports, and more than a third of higher grade intelligence. The thematic EI power provided for in Part 5 of the Bill (which is subject to fewer limitations than the proposed bulk power) has been used at scale to identify dangerous extremists in Syria. Bulk EI is likely to be only sparingly used, and (like thematic EI) will require particularly rigorous and technically-informed oversight. But I have concluded that there is a distinct (if not yet proven) operational case for bulk EI in relation to counter-terrorism, counter-proliferation and cyber-defence.[253]

(d) ***BPDs*** are used on a daily basis, particularly by MI5 and MI6 where internal documents show that they are viewed as "*critical*", "*essential*" and "*fundamental*". We were shown their utility in identifying possible MI6 agents, hostile state actors and potential terrorists, including individuals who posed a threat to the London Olympics and to the UK in the wake of recent attacks in France and Belgium. We also observed how they can be used to exclude large numbers of people from an investigation and to enrich information obtained by other means. The operational case for them is evident.

(e) While ***alternative capabilities*** could sometimes be deployed, including targeted versions of the powers under review and the use of human agents, they were likely to produce less comprehensive intelligence and were often more dangerous (for example to agents and their handlers), more resource-intensive, more intrusive or – crucially – slower. In many cases, there was simply no realistic alternative to use of the bulk power. I concluded that in the great majority of the case studies to which we were introduced, the

252 See chapter 6 above, in particular 6.9-6.11 and 6.44-6.49.
253 See chapter 7 above, in particular 7.10, 7.23-7.26 and 7.32-7.38.

contributions made by bulk powers could not have been replicated by other means.[254]

9.15. A useful recent report on surveillance by the EU's Fundamental Rights Agency quotes the formulation of a distinguished French lawyer which, it is said, "*nicely summarises the difference in approaches to targeted and untargeted surveillance*":

> "Instead of starting from the target to find the data, one starts with the data to find the target."[255]

It is correct that by anomaly detection and pattern analysis, bulk powers have a unique capacity to reveal intelligence about a threat in the absence of any other "*seed*". But as this Report has demonstrated, the uses of bulk powers are not so limited. The powers under review contribute (or, in the case of bulk EI, may be expected to contribute) not only to target discovery, but to target development and to the direction of operations and disruptive action. They are used resourcefully: not mechanically, or in isolation, or for distinct tasks, but in combination with each other and with other types of overt and covert intelligence.

Recommendation

9.16. The making of recommendations in relation to safeguards is specifically excluded from the remit of the Review.

9.17. I have reflected on whether there might be scope for recommending the "*trimming*" of some of the bulk powers, for example by describing types of conduct that should never be authorised, or by seeking to limit the downstream use that may be made of collected material. But particularly at this late stage of the parliamentary process, I have not thought it appropriate to start down that path. Technology and terminology will inevitably change faster than the ability of legislators to keep up. The scheme of the Bill, which it is not my business to disrupt, is of broad future-proofed powers, detailed codes of practice and strong and vigorous safeguards. If the new law is to have any hope of accommodating the evolution of technology over the next 10 or 15 years, it needs to avoid the trap of an excessively prescriptive and technically-defined approach.

9.18. I do however venture to make one major recommendation, again prompted by the speed with which technology can change.[256] It is as follows:

---

254 See 5.20-5.41 (bulk interception), 6.22-6.36 (bulk acquisition), 7.15-7.22 (bulk EI), and 8.15-8.24 (BPDs).

255 EU Agency for Fundamental Rights, *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU* (2015), p.18, quoting M. Delmas-Marty, 'La démocratie dans les bras de Big Brother: Propos recueillis par Johannès, F.', *Le Monde*, 4 June 2015.

The Bill should be amended to provide for a Technology Advisory Panel, appointed by and reporting to the IPC, to advise the IPC and the Secretary of State on the impact of changing technology on the exercise of investigatory powers and on the availability and development of techniques to use those powers while minimising interference with privacy.

I explain my reasoning below.

The impact of changing technology

9.19. It has been apparent to me during the conduct of the Review that though I am clear about the utility (or in the case of bulk EI, potentially utility) of the bulk powers, nothing in this field stays still forever, or even for long. Those authorising, approving and monitoring the exercise of bulk powers need to be alert to technological changes, and their consequences both for the utility of the powers and for the impact of their exercise on individuals.

9.20. To take just a few examples of technological issues that could or should affect the future use of bulk powers (which I offer as theoretical possibilities rather than predictions):

(a) The continuing trend towards universal encryption and anonymisation of devices could reduce the utility of the bulk interception power, or aspects of it (5.55 above).

(b) The future development of a fully-functioning request filter might reduce the operational advantage that the bulk acquisition power currently enjoys over the DRIPA power (6.26-6.28 above).

(c) New techniques for bulk EI will be developed, some of which may disappoint, or show themselves capable of causing unintended damage to devices, and all of which will need to be properly understood by those responsible for authorising them (7.24-7.25 above).

(d) The "*additional promise*" of new techniques for making use of bulk data holdings may bring with it additional threats to the privacy of those whose data is held (8.31(d) above).

The Review was also told by a distinguished independent scientist that the ability to share databases across multiple sites by distributed ledger technology is likely to have its own, perhaps far-reaching, consequences for the exercise of investigatory powers.

---

[256] See also the points made at 2.84 above and fn 257 below.

9.21. A similar emphasis on changing technology was expressed by Matt Tait, who has had relevant experience both inside and outside the SIAs, when he told the Review that:

> "… for the overwhelming majority of the time that the IP Bill will be law, it will be interpreted in secret by HMG lawyers, when seeking to authorise as-yet unknown operations in support of not-yet decided policy objectives, needing to relate the provisions of the IP Bill to technologies that do not exist yet, where technological norms may be markedly different to how they are today …".

That passage underlines the importance of ensuring that authorising and oversight bodies have the requisite technical knowledge not just of current technologies but of present and emerging trends.[257]

9.22. Such knowledge could be transmitted in part by ensuring that warrant applications contain sufficient detail of the methods to be used, and by recourse (should the Judicial Commissioners so choose) to standing counsel to advise them on particularly novel or difficult applications. I would favour both these developments. But it is not sufficient to rely on the necessary understanding being picked up on a case-by-case basis, or through the medium of civil servants and lawyers.

Reducing the privacy footprint

9.23. Also in need of technological expertise are the IPC inspectors whose task it will be to audit the disclosure, retention and use of material acquired pursuant to the new law (clause 205). Are the SIAs' systems equipped with "*privacy by design*",[258] and if not what can be done about it? Could procedures be amended in such a way as to reduce privacy intrusion (for example by greater use of anonymised search results), without jeopardising operational efficiency? Such issues need a practical understanding of how systems are engineered, how powers are operated, and what could be done to minimise the privacy footprint of the SIAs' activities. The Bill already confers duties to audit, inspect and investigate. What is needed in addition is the expertise to enable those duties to be carried out in the most effective possible way.

---

257 It also points up the need to ensure that the IPC "*proactively seeks out and brings to public attention material legal interpretations on the basis of which powers are exercised or asserted*", as the expert lawyer Graham Smith has rightly submitted: supplementary evidence of 22 December 2015 to the Joint Committee on the draft Bill, IPB0126 paras 64-75.

258 Privacy by design is an approach to protecting privacy by embedding it into the design specifications of information technologies, accountable business practices and networked infrastructures: see the "*white paper*" by Canadian Information and Privacy Commissioner A. Cavoukian, *Privacy by Design in Law, Policy and Practice*, 2011.

9.24. Helpfully, the Government has already promised that the IPC will have

> "significantly greater resources, including technical and legal resources, to ensure that they can effectively hold the intelligence agencies and law enforcement to account".[259]

In-house technical resources will plainly be required. But expertise of the kind I have identified will not be easily bought in, for two reasons. First, it requires the expert knowledge and foresight of people who are right at the cutting edge. Secondly, it requires a close understanding of the SIAs' technical and operational systems, plans and ambitions: knowledge which for obvious reasons is very closely held.

The Technology Advisory Panel

9.25. The solution as it seems to me is to provide for a small panel of technology experts – the Technology Advisory Panel **[TAP]**[260] – with very high security clearance, appointed by and reporting to the independent IPC, to support both the IPC and the Secretary of State. The TAP would not be involved in the consideration of warrant applications, but would advise in particular on the technological issues identified above. I see no reason to restrict its range to the four bulk powers which are the subject of this Review.

9.26. Those experts should not be employed by Government or by the SIAs, or have contracts with the SIAs. They should be people who are capable of probing the SIAs, explaining difficult concepts to lay decision-makers, and generally contributing to the culture of robust challenge that will be essential to the effective operation of the IPC. I envisage a mixture of independent academics and individuals with substantial, current experience of industry. I would not disqualify those with a past connection with the SIAs from membership: indeed a degree of understanding of SIA systems and organisation would be of real utility in focusing the work of the TAP where it could be most useful.

9.27. I have considered whether to recommend that one or more moral philosophers submit to vetting for the purpose of serving on the TAP, on the model of the policing panel IDEPP (1.52 above) which I understand has expertise of this kind. The possibility need not be ruled out. But though reflection on the ethical framework for the exercise of investigatory powers can only be desirable, it seems to me that the Judicial Commissioners are in a good position to provide leadership in this area by other means, should they choose to do it, and that the technological expertise of the TAP should not be unduly diluted.

---

259 "Factsheet – Investigatory Powers Commission", published with the draft Bill in November 2015.

260 Not to be confused with the Technical Advisory Board (clause 220), which has a very different function.

9.28. The TAP should have a public profile, perhaps through the IPC rather than a secretariat of its own. The identity of its members would therefore need to be disclosed. It should be encouraged to involve industry, academia and civil liberties organisations in seminars and discussions, and should be fully aware of international developments.

9.29. The TAP would not sit on a permanent basis but could meet several times in a year. So as to focus minds, I would suggest a mandatory annual report to the IPC, furnished also to the Secretary of State, which could be preceded or followed by oral discussions or evidence sessions so as to aid understanding. Other work could be tasked by the IPC as necessary. A full version of the TAP's reports could probably not be made public, but should the ISC require to see them in connection with its own work, access should be granted. The TAP would however remain accountable to the IPC rather than the ISC or the Secretary of State.

9.30. I have been strengthened in my resolve to make this recommendation by learning of the existence (not publicly disclosed until now) of the Scientific Advisory Committees, or SACs, that give external advice to, respectively, MI5/MI6 and GCHQ.[261] Those bodies contain among their members precisely the blend of independent academics and industry experts that it would be desirable to have on the TAP. Subject to avoiding any possible conflicts of interest, the Chief Judicial Commissioner might choose to recruit past or current members of the SACs to serve on the TAP. I was able to discuss the idea with the current Chair of one of the SACs, whose preliminary reaction was positive.

9.31. The point of the TAP would not be to provide an alternative oversight function, or to place new regulatory burdens on the SIAs. Rather, it would serve to inform the Secretary of State, and enhance the work of the IPC, by ensuring that both are kept as up to date as possible with the fast-moving technologies whose use they are asked to approve (and, in the case of the IPC, to audit).

9.32. This Report has declared the powers under review to have a clear operational purpose. But like an old-fashioned snapshot, it will fade in time. The world is changing with great speed, and new questions will arise about the exercise, utility and intrusiveness of these strong capabilities. If adopted, my recommendation will enable such questions to be answered by a strong oversight body on a properly informed basis.

[261] See 1.42 above.

ANNEXES

ANNEX 1

LIST OF ACRONYMS/ABBREVIATIONS

List of Acronyms / Abbreviations

2015 ISC Report	March 2015 report of ISC: see fn 16
2016 ISC Report	February 2016 report of ISC: see fn 29
AQOT	A Question of Trust, Report of June 2015
the Bill	Investigatory Powers Bill 2016
BPD	Bulk Personal Dataset
Bulk EI	Bulk Equipment Interference
CD	Communications Data
CDI	Content-derived information
CHIS	Covert Human Intelligence Source
CJEU	Court of Justice of the European Union
CNE	Computer Network Exploitation
COBR	Cabinet Office Briefing Room (emergency response committee)
CPS	Crown Prosecution Service
CSP	Communications Service Provider
DR	Dissident Republican (Northern Ireland)
DRIPA 2014	Data Retention and Investigatory Powers Act 2014
DSOU	Don't Spy on Us Coalition
DV	Developed vetting
ECHR	European Convention of Human Rights
ECtHR	European Court of Human Rights
EI	Equipment Interference
EU	European Union
FBI	Federal Bureau of Investigation (USA)
FISA	Foreign Intelligence Surveillance Act (USA)
FISC	Foreign Intelligence Surveillance Court (USA)
GCHQ	Government Communications Headquarters
ICRs	Internet connection records
IDEPP	Independent Digital Ethics Panel for Policing
IOCC	Interception of Communications Commissioner
IOCCO	Interception of Communications Commissioner's Office

IP	Internet Protocol
IPC	Investigatory Powers Commission
IPT	Investigatory Powers Tribunal
ISA 1994	Intelligence Services Act 1994
ISAF	International Security Assistance Force (NATO force in Afghanistan)
ISC	Intelligence and Security Committee of Parliament
IsComm	Intelligence Services Commissioner
ISIL	Islamic State of Iraq and the Levant (so-called)
LPP	Legal Professional Privilege
MI5	Security Service
MI6	Secret Intelligence Service
NAS Report	US National Academy of Sciences Report, 2015
NCA	National Crime Agency
NCND	Neither confirm nor deny
NGO	Non-Governmental Organisation
NSA	National Security Agency (USA)
PCLOB	Privacy and Civil Liberties Board (USA)
PPD-28	Presidential Policy Directive 28
PSNI	Police Service of Northern Ireland
RAS	Reasonable, articulable suspicion (USA)
RCD	Related Communications Data
RIPA 2000	Regulation of Investigatory Powers Act 2000
RUSI	Royal United Services Institute
SAC	Scientific Advisory Council
SIAs	Security and Intelligence Agencies (MI5, MI6 and GCHQ)
SIGINT	Signals Intelligence
SOI	Subject of Interest
SSA 1989	Security Service Act 1989
TA 1984	Telecommunications Act 1984
TAP	Technology Advisory Panel
VOIP	Voice Over Internet Protocol
WTA 2006	Wireless Telegraphy Act 2006

ANNEX 2

TERMS OF REFERENCE

Independent review of the operational case for bulk powers: Terms of Reference

Aim

1. The review will examine the operational case for the investigatory powers contained in Parts 6 and 7 of the Investigatory Powers Bill, including the 'Operational Case for Bulk Powers' document which was published alongside the Bill at Introduction on 1 March. The review will report to the Prime Minister, with a copy sent to the Intelligence and Security Committee of Parliament (ISC). It will build on the previous reviews by the ISC, David Anderson QC and the Surveillance Panel convened by the Royal United Services Institute. The review will inform Parliament's consideration of the need for the bulk powers in the Bill.

2. The review shall consider the operational case for:

i. Bulk Interception
ii. Bulk Equipment Interference
iii. Bulk Acquisition (Communications Data)
iv. Bulk Personal Datasets

Process

3. The review will be undertaken by David Anderson QC, supported by a security-cleared barrister, technical expert and a person with experience of covert investigations.

4. The Government and the Security and Intelligence Agencies will provide all necessary information, access and assistance as is needed for David Anderson QC to undertake his review effectively.

5. David Anderson QC will report to the Prime Minister on the findings of his review in time for those findings to inform Lords Committee consideration of Parts 6 and 7 of the Bill. A copy of the report should also be provided to the ISC at this time. The Prime Minister will make the final decision as to whether the report, or parts of it, can be published without prejudicing the ability of the Security and Intelligence Agencies to discharge their statutory functions. There may be a classified annex that should also be submitted to the Prime Minister and copied to the ISC.

ANNEX 3

EXCHANGE OF LETTERS

Letter of 6 June 2016 from Keir Starmer QC MP to Rt Hon John Hayes MP, Minister of State for Security

Dear John,

Re: Investigatory Powers Bill, Independent Review of bulk powers

Following our recent discussions about the independent review of bulk powers, I thought it would be helpful to clarify the basic framework of the review.

As we have discussed the review will:

(a) Be carried out by David Anderson QC supported by a security cleared barrister, a technical expert and a person with experience of covert investigations.

(b) Examine the operational case for the bulk powers in the Bill, not merely in respect of the utility of the powers, but also their necessity.

(c) Have access to all necessary information as is needed to undertake the review effectively, including all information provided to the Intelligence and Security Committee.

(d) Take about three months to complete and will report to the Prime Minister in time for the findings to inform Lords Committee considerations of Parts 6 and 7 of the Bill.

I would be grateful if you could indicate that this is the agreed basic framework for the review as soon as possible.

Yours sincerely,

Keir Starmer MP

Shadow Home Office Minister and MP for Holborn & St Pancras

Response of 6 June 2016 from Rt Hon John Hayes MP, Minister of State for Security, to Keir Starmer QC MP

Dear Keir,

Thank you for your letter of earlier today regarding the review of the operational case for bulk powers, which will be announced tomorrow during Report stage of the Investigatory Powers Bill. I can confirm that the basic framework for the review will be as set out in your letter.

On your point about the composition of the review team, you are quite right that the team will consist of a security cleared barrister who has significant experience working as a special advocate against the Government in terrorism cases, a technical expert who supported David on his investigatory powers review, and a former senior law enforcement officer with significant operational experience and knowledge of the use of a wide range of investigatory techniques. David Anderson has hand-picked his team and we are confident that together they have the range and depth of knowledge needed to undertake a comprehensive review.

In relation to your second point, it is absolutely the case that this review will be addressing the specific question of whether the bulk capabilities provided for in the Bill are necessary. The review team will critically appraise the need for bulk capabilities, which will include an assessment of whether the same result could have been achieved through alternative investigative methods.

On your third point, the Terms of Reference for the review makes clear that the Government and Security and Intelligence Agencies will provide David Anderson and his team with all necessary information, access and assistance as is needed for the review to be undertaken effectively. We are absolutely clear that there is nothing to be gained, and much to be lost, by in any way restricting the review team's access to sensitive and classified material where this is necessary to inform the review process.

On the issue of timing, you are correct that the review will be concluded in time to inform Parliament's consideration of Parts 6 and 7 of the Bill at Lords Committee. We are confident that David Anderson and his team will have the necessary time and resources to undertake a detailed assessment of the necessity of these provisions.

Thank you for the opportunity to provide these binding assurances.

The Rt Hon John Hayes MP

ANNEX 4

STRUCTURED DESCRIPTION OF INTELLIGENCE WORK

STRUCTURED DESCRIPTION OF THE STAGES OF SECURITY AND INTELLIGENCE WORK, AND SPECIFIC ACTIVITIES UNDERTAKEN WITHIN THESE STAGES

(Supplied to the Review by MI5, MI6 and GCHQ: June 2016)

DEFINITIONS

Introduction

This note has been put together to provide a consistent structure and terminology for discussions about the way in which the Security and Intelligence Agencies (SIA) make use of bulk data in pursuit of their statutory functions. There have been a range of studies conducted on both sides of the Atlantic which have used different terms to describe identical activities, and conversely identical terms to describe different activities. Furthermore there are words that are used in the public debate which have a specific technical or legal meaning within the SIA ("surveillance" being the most obvious example). By setting out a high-level structured description of the stages of security and intelligence work, and the specific activities undertaken within these stages, we hope to facilitate discussion.

Stages of Security and Intelligence Work

The work of the Agencies can be broken down into three stages. In any given investigation, and certainly in the sustained production of intelligence to meet a particular intelligence priority, these stages are not followed in a strictly linear way. Most of the time there will be elements of all three in train. Nonetheless we consider that the three stage model provides a useful basis for considering how bulk data is used.

1. IDENTIFY

   This is the process by which initial "seed" information is analysed and developed to the point where it is clear that there is e.g. a potential terrorist threat, a possible candidate for recruitment as an agent, or a source of exploitable intelligence meeting current requirements. The initial "seed" information may come from anywhere: open source (a tweet claiming responsibility for an activity, say); a humint tip-off; forensic data from seized media; information from a foreign liaison partner. Bulk data is vital at this stage in the process and may often be one of the only sources of information available to the Agencies.

2. UNDERSTAND

   This is the process by which the intelligence picture is developed and enriched to the point where decisions can be taken about resourcing and prioritisation. Bulk data is used to help assess potential threats and opportunities, and where appropriate to seek authorisation for targeted intelligence collection to supplement bulk data.

3. ACTION

   This stage encompasses a wide range of activities, which bulk data will have helped to inform. The output of the "identify" and "understand" phases might be the production of intelligence reports, the running of a recruitment operations, or the launching of disruption activity whether through arrests to prevent a e.g. terrorist attack plan or on-line "effects" operations.

Activities

The specific activities conducted by analysts within the Agencies will include the following:

- Target discovery – identifying individuals who may be subjects of intelligence interest from lead intelligence.

- Target development – enriching understanding of a subject of intelligence interest, their connections, networks and patterns of activity, in order to understand potential threat or opportunities.

- Anomaly detection – a technology-based process by which patterns in bulk data are identified and analysed to assist in the detection of e.g. malware and cyber-attack signatures. This is essential for Cyber Defence.

- Network Analysis – this is a technology-based process by which information is gathered from interception to develop understanding of the network environment to provide context to the intercepted data and enable more effective operation of e.g. the bulk interception process.

- Triage and prioritisation – at all stages bulk data helps to inform decisions about prioritisation of resources by the Agencies, including the allocation of scarce technical, analytic, human or other collection resources.

ANNEX 5

STATEMENT OF UTILITY OF BULK CAPABILITIES (MI5)

MI5 STATEMENT OF UTILITY OF BULK CAPABILITIES

(supplied to the Review July 2016)

Bulk capabilities are critical to the work of MI5: over the last decade they have enabled us to work securely at both the scale and pace that we need to protect national security. As we adapt to the challenges posed by technological change, for example the increasing proliferation of communications data and apps, many subject to sophisticated encryption, bulk data – alongside our other capabilities – is increasingly important to us. All of our investigators and data analysts across all of MI5's areas of operations use bulk capabilities to ***identify*** threats, ***understand*** them and to inform ***action***:

- ***International Counter Terrorism:*** ISIL is pursuing a global terrorist campaign threatening UK citizens at home and overseas. It has a proven intent and capability to conduct large-scale attacks in Europe. Bulk data has played a significant part in every major counter terrorism investigation of the last decade, including in each of the seven UK attack plots disrupted since November 2014.

- ***Northern Ireland Related Terrorism:*** Dissident Republican (DR) groupings continue to conduct attacks designed to kill members of the security forces including police and prison officers. In 2015 there were 16 DR attacks, and in 2016 Prison Officer Adrian Ismay died as a result of such an attack. Bulk capabilities are essential to understanding the plans of resilient, experienced terrorists and stopping their attacks.

- ***Hostile Foreign Activity:*** The UK is a priority espionage target for hostile foreign actors. The volume and complexity of cyber-attacks has risen sharply, posing growing risks to our critical national infrastructure. The high level of sophistication and communications security used means that bulk capabilities, including through joint working with GCHQ, are critical to identifying and mitigating threats.

Bulk capabilities are not about monitoring the activities of innocent members of the public: they are a vital tool in keeping the UK safe. They have undoubtedly helped save lives.

Identify

- MI5 receives hundreds of new leads every week, often containing only fragments of information about a threat. Leads come from a wide range of sources, including from GCHQ and SIS, from agents, or from partner services. It is essential that leads are rapidly progressed. We use Bulk Personal Data to quickly develop fragmentary intelligence into a real world identity, and Bulk Communications Data can be used to identify links to known targets and activities of interest.

- This means that we can quickly identify and open investigations to thwart activities that pose a threat, for example a terrorist travelling from Syria to the

UK, or a group planning attacks. This enables us to identify those individuals who pose a threat, and to avoid intruding into the privacy of those who don't, like individuals who might be subject to malicious accusations. Without bulk capabilities, MI5 simply could not effectively process and respond to the volumes of incoming leads.

Understand

- At any one time MI5 is running several hundred complex and fast-moving investigations. Bulk capabilities are essential to understanding and prioritising targets, so that we can focus our finite resource on those who pose the greatest threat.

- MI5 uses Bulk Personal Data and Bulk Communications Data on a daily basis to understand target behaviour: identifying target communications, travel patterns and links between plotters, and enabling us to "*join the dots*". Bulk Personal Data and Bulk Communications Data also complement our targeted collection: identifying new communications devices which may be subject to further targeted enquiries, keeping our human sources safe and ensuring intrusion is always kept to a minimum. Without bulk capabilities we could not prioritise or manage risk at the necessary pace and scale.

Action

- MI5 uses Bulk Capabilities to find out the plans of those who mean us harm so that we can take action and stop them. Bulk capabilities identify attack operatives we know have been deployed by ISIL and other terrorist groups and can also alert us to changes in behaviour indicating an attack is imminent. Bulk Communications Data and Bulk Personal Data enable MI5 and the police to take disruptive action and stop attacks: bulk capabilities have undoubtedly helped to save lives.

  We are clear that our reliance on all of the bulk powers we, and our partners, currently use is becoming ever more important to us in identifying threats and building the intelligence picture around them, in the face of the challenges posed by encryption. This is likely to remain the case for the foreseeable future.

ANNEX 6

STATEMENT OF UTILITY OF BULK CAPABILITIES (MI6)

MI6 STATEMENT OF UTILITY OF BULK CAPABILITIES

(supplied to the Review July 2016)

SIS uses its bulk investigatory powers to identify and understand threats to the UK and intelligence opportunities in an overseas context. We live in a data-led world; to maintain an edge over the UK's adversaries SIS requires appropriate and safeguarded access to that data. The people who assist SIS globally to keep the UK safe and prosperous often possess rare qualities and talents. Finding them and keeping them safe is helped greatly through the use of bulk powers.

SIS often depends on the use of bulk powers by GCHQ and MI5 to provide the seed of information which it can then develop and enrich through its own use of bulk powers.

- ***Bulk Personal Datasets:*** Bulk personal datasets make a valuable and significant contribution to SIS activity and they often form the backbone of investigative work. Around 80% of people working on intelligence operations in SIS have access to bulk personal datasets. These datasets enable SIS to take a piece of fragmentary information and make a positive identification of a person of intelligence interest who otherwise could not be identified. Such datasets also help SIS to better understand the risks surrounding its activities in order to protect the people it works with all over the world. Bulk personal data is equally important across all operational areas covered by SIS including counter-terrorism, counter-proliferation, cyber, serious crime and the geographical requirements for intelligence collection as set out in the National Security Strategy. Its importance to SIS is likely to increase.

- ***Bulk Interception***: SIS depends on GCHQ's use of bulk interception to provide targeted information that can then be developed by SIS to understand intelligence threats and opportunities. Without this, SIS operations across all areas (counter-terrorism, counter-proliferation, cyber, serious crime and geographical requirements for intelligence collection) would be significantly damaged, including the ability to understand operational risks and manage them appropriately. Its importance to SIS is unlikely to decline.

- ***Bulk Acquisition of Communications Data***: SIS depends on GCHQ's and MI5's use of bulk acquisition of communications data to develop an understanding of a threat to the UK, which SIS can then use its assets and capabilities to inform and disrupt. This is particularly important in the context of counter-terrorism. Its importance to SIS is unlikely to decline.

- ***Bulk Equipment Interference:*** SIS is likely to become increasingly dependent on GCHQ's use of bulk equipment interference to identify threats to the UK. This will allow SIS to develop further the understanding of these threats and take steps to disrupt them. This is likely to be particularly important in the context of counter-terrorism and cyber. Given the increasing use of encryption and diversity of communication methods, the importance of this bulk power to SIS is likely to increase.

ANNEX 7

STATEMENT OF UTILITY OF BULK CAPABILITIES (GCHQ)

GCHQ STATEMENT OF UTILITY OF BULK CAPABILITIES

(supplied to the Review July 2016)

GCHQ would not be able to identify those who wish us harm without bulk powers. Terrorists, child abusers, drug traffickers, weapons smugglers and other serious criminals choose to hide in the darkest places on the internet. GCHQ uses its bulk powers to access the internet at scale so as then to dissect it with surgical precision.

By drawing out fragments of intelligence from each of the bulk powers and fitting them together like a jigsaw, GCHQ is able to find new threats to the UK and our way of life; to track those who seek to do us harm, and to help disrupt them.

- ***Bulk Interception:*** Interception provides valuable information that allows us to discover new threats; it also provides unique intelligence about the plans and intentions of current targets – through interception of the content of their communications. Communications data obtained through bulk interception is also crucial to GCHQ's ability to protect the UK against cyber-attack from our most savvy adversaries and to track them down in the vast morass of the internet.

- ***Bulk Acquisition of Communications Data:*** Together with communications data obtained through bulk interception, this power is the primary way in which GCHQ discovers new threats to the UK. Without it, these threats would develop to fruition undetected until it was too late to stop them.

- ***Bulk Equipment Interference:*** The increasing use of encryption and diversity of communications methods means that bulk EI is of growing importance. It can enable GCHQ to "*overcome techniques used by targets to hide their identities or their communications*". "*CNE can be a critical tool in investigations into the full range of threats to the UK from terrorism, serious and organised crime and other national security threats. For example, CNE enables the state to obtain the valuable intelligence it needs to protect its citizens from individuals involved in terrorist attack planning, kidnapping, espionage or serious organised criminality.*"[262]

- ***Bulk Personal Datasets:*** GCHQ uses bulk personal datasets in conjunction with other powers to identify new targets and to enrich our knowledge of existing targets – for example, by confirming their identity, or discovering new connections and networks.

What follows is a more detailed breakdown of the utility of each power by activity type and operational area.

[262] The quotations are taken from the first witness statement of Ciaran Martin, dated 16 November 2015, in *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and GCHQ* [2016] UKIPTrib 14_85-CH, para 26. [DA to check para no. of first quote]

Is the power gaining or declining in importance?

Identify

It is GCHQ's ability to interrogate the communications data obtained through bulk interception that provides the key capability to answer questions about developing incidents as they occur and identify the individuals involved. Much of the information needed to produce this intelligence is often drawn from a composite of individual pieces of data that occur weeks or even months before the event takes place. This information can inform us about location, contacts of our adversaries or aspects of their behaviour through technology, but also provides GCHQ with the assurance that an account targeted for more intrusive content collection does not belong to a UK individual.

- ***Interception – remain the same / decline***
- ***EI – increasing***
- ***BPD – increasing***
- ***CD – remain the same***

Understand

Interception and EI can provide (sometimes real time) intelligence on the "*plans and actions of individual terrorists, criminals and other targets, which can be used to disrupt or frustrate their plans*".[263] These capabilities can also be used to identify other previously unknown communications of existing targets – for example a new phone or email address. "*The age of ubiquitous encryption means, inter alia, that GCHQ ... require[s] a more innovative and agile set of technical capabilities to meet the serious national security challenges of the digital age. Computer and Network Exploitation [CNE] is one such capability.*"[264]

- ***Interception – remain the same for cyber defence / decline for non-cyber defence***
- ***EI – increasing***
- ***BPD – remain the same for GCHQ***
- ***CD – remain the same / decline***

Action

For GCHQ, it is the output of analysis of the information obtained under the bulk powers that is used at this stage, rather than the powers themselves. GCHQ works with and in support of the other Agencies – for example in direction support of MI5 counter-terrorism investigations, or assisting SIS with Agent recruitment, and provides them with intelligence based on information obtained using the bulk powers. It is true to say that all of the bulk powers are

263 Witness statement of Charles Farr in *Liberty v Secretary of State for the Foreign and Commonwealth Office and others* [2014] UKIPTrib 13_77-H, para 31.

264 Witness statement of Ciaran Martin in *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and GCHQ* [2016] UKIPTrib 14_85-CH, para 20.

valuable to GCHQ at this stage, whether singularly, together or when combined with other, more targeted techniques.

- ***Interception – remain the same for cyber defence / decline for non-cyber defence***
- ***EI – increasing***
- ***BPD – remain the same for GCHQ***
- ***CD – remain the same / decline***

By operational area[265]

The utility of the bulk powers is the same across the majority of GCHQ's operational areas. For ***geo-political*** teams (including ***economic security, weapons and counter-proliferation***), ***Serious Crime, Cyber Defence*** and ***Counter Terrorism***, the ability to use bulk powers to identify and understand our adversaries relies on a combination of the bulk powers. Bulk interception remains an important capability, and the importance of bulk equipment interference will increase in the coming years. Both the bulk acquisition of communications data and bulk personal datasets allow GCHQ to minimise intrusion into privacy when seeking to identify new leads and can also be used to provide GCHQ with the assurance that an account targeted for more intrusive content collection does not belong to a UK individual.

Additionally, for ***geo-political*** teams and ***serious crime***, the bulk powers can also be used to identify other previously unknown communications of existing targets – for example a new phone or email address – and can provide valuable intelligence on the plans and actions of subjects of interest.

For our work in support of ***counter terrorism***, it is GCHQ's ability to interrogate the communications data obtained through bulk interception that provides the crucial capability to answer questions about developing incidents as they occur and identify the individuals involved.

"*We have examined cases which demonstrate that [bulk interception] has been used to find communications indicating involvement in threats to national security. Bulk interception has exposed previously unknown threats or plots which threatened our security and which would not otherwise have been detected.*"[266]

Communications data obtained through bulk interception is crucial to GCHQ's ability to protect the UK against cyber-attack from our most savvy adversaries and to track them down in the vast morass of the Internet (***Cyber Defence***).

"*The speed of events in cyber space and the vast size of the internet limit the utility of more targeted powers and make bulk capabilities essential to the UK's efforts to detect and defend against such attacks. 95% of the cyber-attacks on the UK detected by the agencies over the last six months were only discovered through the collection and analysis of bulk data.*"[267]

---

265 [Areas taken from allocation of effort breakdown in ISC Annual Report, 2015-16 (5 July 2016).]

266 2015 ISC Report, Overview para x.

267 [Attribute quote: GCHQ to provide reference to "OCBP"].

Overall we assess the following direction of travel for the utility of each of the bulk powers.

- **Interception – remain the same for cyber defence / decline for non-cyber defence**
- **EI – increasing**
- **BPD – remain the same for GCHQ**
- **CD – remain the same / decline**

ANNEX 8

CASE STUDIES – BULK INTERCEPTION

CASE STUDIES
BULK INTERCEPTION

Case study A8/1

GCHQ
Bulk interception/bulk acquisition data
Action[268]
Counter-terrorism

In 2015, GCHQ analysts used communications data obtained under bulk interception warrants to search for potential new phones used by individuals known to be involved in plotting terrorist acts in the UK. Following the identification of a new phone number, GCHQ conducted further analysis to identify contacts and additional 'selectors' being used by the same individual. Subsequent analysis, combining communications data obtained under bulk interception warrants and communications data acquired under s94 TA 1984, enabled GCHQ to identify an operational cell. Further to this, the analysis of the content of communications and other, more targeted techniques revealed that the cell had almost completed the final stages of a terrorist attack. The police were able to disrupt the plot in the final hours before the planned attack.

GCHQ provided the Review team with intelligence reporting which showed that, without access to bulk data, GCHQ would not have been able to complete this work at all; the exposure of the operational communications was made possible only because GCHQ analysts were able rapidly to develop the contacts of every phone in the network as they investigated. GCHQ staff explained that, on its own, each phone would not necessarily have been identified as suspicious but, when taken as a network, the likely operational nature of the phones was clear to see.

In this case, the SIAs had no other leads to follow.

GCHQ managers told the Review team that the ability to identify operational phones through analysis of bulk data had been crucial in a number of similar operations.

[268] In each case study I have highlighted the nature of the principal work involved, by reference to the SIAs' Structured Description of Intelligence Work (Annex 4).

Case study A8/2

GCHQ/MI5
Target development/pattern analysis
Counter-terrorism
Summarised in *A Question of Trust Annex 9 Case Study 3*

This case study relates to events in 2009. After the disruption of a UK terrorist cell, GCHQ and MI5 continued to investigate the potential overseas links of that cell as a high priority.

GCHQ staff told the Review team that analysis of secondary data obtained through bulk interception warrants proved critical to the discovery of a new UK-based terrorist plot. GCHQ undertook complex analysis of this data to look for patterns of behaviour indicative of operational planning. They identified an email address that was in contact with a UK-based individual. Analysis of the communications data and content of these emails revealed more members of the UK network and details of the attack plot. The UK individual was subsequently arrested along with a number of associates. Without bulk data, GCHQ would not have found the email addresses which led to the identification of the UK-based operative.

Case study A8/3

GCHQ/MI5 and partner agencies
Identify/triage/target discovery and development
Counter-terrorism

Following terrorist attacks in France, GCHQ provided support to both MI5 and European partners in identifying targets and prioritising leads. GCHQ triaged around 1600 international leads (in the form of telephone numbers, email addresses or other identifiers) in the days following the attacks. It was necessary quickly to determine whether there was any further attack planning or to rule out the possibility of further attacks.

GCHQ used both secondary data and content obtained through bulk interception warrants to identify those leads that should be prioritised for further investigation by intelligence and law enforcement partners.

Without bulk data, this triage work would have taken much longer and GCHQ would have needed to make targeted requests in relation to each potential lead. In most cases, they would have had to relay these requests to overseas CSPs through foreign partners. This approach would potentially have taken many months and would inevitably have led

to GCHQ obtaining an incomplete picture where such partnerships were unavailable or ineffective in obtaining the necessary data. As a result, GCHQ would have been able to provide only limited assurance that possible further attack planning had been identified or ruled out.

Further analysis enabled GCHQ to identify other extremists, based in Syria and suspected of planning terrorist attacks against the West. Ongoing development, using data obtained under bulk interception and other intelligence community capabilities, has formed an important part of UK and European partners' knowledge and understanding of these attacks in France.

The Review team was given details which demonstrated that, without the ability to interrogate secondary data obtained through bulk interception, GCHQ would not have obtained any of the intelligence derived from this lead.

Case study A8/4

GCHQ
Identify/target discovery and development
Counter-terrorism
Summarised in *A Question of Trust Annex 9 Case Study 2*

In this 2009-2010 operation, GCHQ used bulk data to identify, and monitor the activity of, a senior Al Qaida leader and his network in a Middle Eastern country; they had been behind a plot to attack Western interests. These individuals went to great lengths to try to hide their communications; the use of bulk data was vital to GCHQ's work in keeping track of them. Ultimately, the interrogation of this bulk data led to the identification of an individual in the UK who, it transpired, had offered to use his access to an airport to launch a terrorist attack from the UK. Following an investigation, he was convicted on terrorism charges.

Case study A8/5

GCHQ
Identify/target discovery and development/action
Counter-terrorism
Summarised in the Operational Case and *A Question of Trust Annex 9 Case Study 3*

Many Syria-based extremists with links to the UK and the West, including those involved in attack planning, make sophisticated efforts to avoid detection by the SIAs. The interrogation of bulk data is the principal tool used by GCHQ's counter-terrorism analysts

to identify and maintain coverage of these individuals in order to know whether they are actively planning terrorism operations.

In 2013, analysis of secondary data, obtained under bulk interception warrants, uncovered a previously unknown email account in contact with a Syria-based extremist suspected of involvement in planning attacks against the West. Further analysis of secondary data revealed that the user of this newly discovered email account was attempting to hide his true intentions. Bulk interception allowed GCHQ to maintain coverage of his activities despite these attempts.

Analysis of the content of the communications revealed that he was leaving Syria and travelling to Europe for the next stage of his attack planning. This information was passed to the authorities of the country to which he had travelled. They took steps to disrupt his activities.

The Review team was shown some of the intelligence reports created in 2014 as links with the suspect were developed. The team was given details which showed that it is very unlikely that the individual would have been identified without the use of bulk interception.

Case study A8/6

GCHQ
Action
Support of military operations

The Review team was told that, during the Afghanistan campaign, UK military forces were deployed on multiple occasions to counter insurgent and terrorist activity. Their tasks included the rescue of UK nationals. Such operations could depend upon intelligence from bulk interception to locate the targets and assess the right moment for military intervention.

In one case, around 50 members of GCHQ provided 24/7 support to teams on the ground in an operation to find and rescue a number of individuals who had been taken captive. Analysis of secondary data acquired through bulk interception enabled GCHQ to gather intelligence about the armed group, and then quickly to deploy more intrusive techniques in order to gain insight into the group's intent. This work enabled GCHQ to locate the group, monitor it and establish the group's links with known terrorist networks. Within 72 hours of the kidnapping, the hostages had been located. Analysis of the content of the communications of the kidnappers, obtained through bulk interception, indicated that the hostages' lives were in imminent danger. This information was passed

swiftly to a COBR meeting and the Prime Minister authorised a rescue attempt by UK military forces. The hostages were subsequently successfully rescued.

In this case, the Review team is unaware of any likely alternative method to bulk interception through which the hostage-takers could have been identified and located, or their intentions revealed, sufficiently swiftly to ensure the safety of the hostages.

GCHQ managers explained to the Review team that they would not be able to respond to the majority of hostage cases without bulk interception. In most cases (as in this example), GCHQ has to start from scratch, with no existing intelligence to assist. The use of bulk interception is the only means to achieve the quick results that are needed in hostage situations.

Case study A8/7

GCHQ
Action
Support of military operations

During the Afghanistan campaign, Camp Bastion in southern Afghanistan was the main base for UK military forces. It was considered a top target by the Taleban who continually made attempts to attack the base and those within it.

As part of its support to military operations and force protection, GCHQ used analysis of secondary data obtained under bulk interception warrants to identify mobile devices in the area of Camp Bastion; where those devices were in contact with known insurgents, GCHQ then prioritised the devices for further analysis. It quickly became clear from subsequent bulk interception that what had been uncovered was extensive planning involving multiple insurgents.

Bulk interception gave GCHQ access to the content of the insurgents' communications; this led to the identification of further members of the group and to the discovery of details of attack planning, including a plan to mount a co-ordinated attack against Camp Bastion. The information was passed to those responsible for security at the Camp and enabled British forces to disrupt several planned attacks.

This support to the UK military would not have been possible without the use of both secondary data and content obtained under bulk interception warrants. In circumstances like those in Afghanistan at this time, there was no practical means to obtain communications on a purely targeted basis; the only way to obtain communications was to piece them together from the global communications network under a bulk authority.

While sometimes alternative sources, such as a tip off, might have alerted ISAF forces to an imminent attack, no such information was available in this instance. Bulk interception was the only means through which the UK was alerted to the intended attack.

Case study A8/8

GCHQ
Action/anomaly detection
Cyber-defence

GCHQ used bulk interception in order to identify malware placed on a nationally important UK computer network by an overseas-based organised crime gang who controlled a particularly sophisticated piece of malware.

The malware was initially identified by financial institutions as a potential threat. By looking for traces of this malware within the bulk data available to GCHQ, analysts were able to obtain a more accurate understanding of the scale of the attack and the risk posed to the UK. Further GCHQ analysis of bulk data identified the infrastructure being used by criminals to deploy and control the malware. GCHQ was able to alert the users and also to monitor the success of the cyber-defences then put in place by those users.

The information obtained by GCHQ allowed law enforcement officers subsequently to take action and arrest members of the organised crime gang.

It is possible that commercial anti-virus companies might have been able to provide some defence against the attack, if appropriate software had been installed on the devices under attack. However, commercial companies would not have been able to identify the overseas attackers nor to provide information to potential victims in advance of an attack. An industry view will be on a customer-by-customer basis and will not provide a picture of the overall threat to the UK.

By analysing secondary data obtained under bulk interception warrants, GCHQ can identify the overseas-based criminals behind significant malware threats and the key computer network infrastructures that they are using. GCHQ told the Review team that there is a high volume of criminal cyber threats in circulation, and that the National Crime Agency (NCA) needs to identify those who pose the most significant danger to citizens and the broader UK economy. GCHQ analysis of bulk communications data helps the NCA to mitigate these threats, informing and enabling disruption activity against them. GCHQ currently deals with over 200 cyber incidents every month.

Case study A8/9

GCHQ
Action/anomaly detection
Cyber-defence

In 2016 a European media company suffered a major, destructive cyber-attack. Through the analysis of bulk interception data, GCHQ was able to link this attack to other compromises in the same sector and to explain what had happened. Further information then suggested a possible imminent threat to the UK from the same cyber attackers during the UK election period. GCHQ deployed a capability to protect government networks from this cyber attacker, and media organisations were briefed to enable them to protect their networks. Since then, a particular UK media company has been alerted to a compromise by the same attackers and has been able to clean up its networks. The combination of the analysis of communications data obtained through bulk interception data and work with international partners helped to prevent the UK from suffering a major attack similar to that on the European company.

To achieve the same outcome without the use of bulk powers, GCHQ would have had to place sensors on the computers of thousands of potential victims, which would not have been practical and would not necessarily have been effective. Since there had been no reason to believe that the UK media company would be selected for a cyber-attack, the attack would not have been detected by targeted means. It is possible that commercial anti-virus companies might have been able to provide some defence against the attack, if the media company had had appropriate software installed. However, as in the previous example, a commercial provider would not have been able to provide advance warning or identify the overseas attackers. Further, whether or not a business has protection against such an attack depends, inevitably, upon whether that business has chosen to buy cyber-defence products.

Cyber-defence analysts use bulk interception to detect attacks; attacker infrastructure is located across the world and changes constantly. In addition, attackers have a wide range of targets – governmental, military, economic, industrial and commercial – and GCHQ cannot predict in advance which entities will be targeted or when they will be targeted. GCHQ therefore cannot provide adequate cyber-defence through targeted means.

GCHQ estimates that 60% of those victims whom it has identified as having been the subject of cyber-attack did not know that they had been targeted. Since some companies may choose for commercial reasons not to publicise the fact that they have suffered a cyber-attack, and since GCHQ cannot say that it has identified every victim, the true percentage of all victims may be different.

Case study A8/10

GCHQ
Action
Child sexual exploitation
Summarised in the Operational Case

The Review team was given details of an extensive operation targeting those involved in child sexual exploitation (CSE) online. GCHQ managers told the Review team that its ability to analyse secondary data gained from bulk interception has provided significant new insight in recent months into the nature and scale of the online CSE threat to the UK. In April 2016 alone, GCHQ identified several hundred thousand separate IP addresses worldwide being used to access indecent images of children on the open web. This figure is only a snapshot, and does not include access to such images through the dark web.

This insight has challenged some of the UK's existing thinking and plans as to how to counter online CSE. GCHQ has also used the same capability to analyse secondary data to assist the National Crime Agency (NCA)'s efforts to prioritise online CSE leads, for instance of those whose online behaviour suggests they pose the greatest risk of committing physical or sexual assaults against children. The Review team was told that, in seeking to identify users who should be investigated as a priority, GCHQ uses criteria that were developed by academics, law enforcement agencies and charities. The team was given two examples of arrests made as a result of GCHQ's CSE work.

One of those arrested was an individual who operated anonymously online to avoid detection. After he used a VOIP provider to contact another suspect who was already under investigation, the NCA prioritised the investigation of his activities. Despite full co-operation from the service provider, attempts to identify him were unsuccessful. Although the NCA had discovered the anonymous online user name he had used, the details that he had used to register them did not allow him to be tracked back to his "real world identity" using conventional means.

GCHQ analysts applied advanced analytic techniques to secondary data that had been obtained under bulk interception warrants and was held within GCHQ databases. The analysts rapidly identified recent online activity by the individual and a number of current contact details. These were passed to the NCA which was then able to obtain a genuine name and address for the individual, leading to a swift arrest. The individual pleaded guilty to multiple charges, including two counts of sexual abuse, and received a custodial sentence of over 3 years as a result.

While it might be possible partially to replicate some of this work by requesting data from CSPs (both in the UK and overseas), these means would be likely to result in a far less

accurate overall picture and would not be as effective as the use of bulk interception in identifying technologically-sophisticated individuals engaged in online CSE. As in this example, individuals often use false details to avoid identification and also use multiple communications methods. It would take significantly more time to obtain results, delaying the safeguarding of children and giving the offender more time to target more victims.

Case study A8/11

GCHQ
Action
Child sexual exploitation
Summarised in *A Question of Trust Annex 9 Case Study 5*

GCHQ analysis of bulk interception identified two individuals in Kuwait who were using social media to groom and blackmail over 100 children, the majority of whom were in the UK. These individuals forced children into producing self-generated indecent imagery.

Before GCHQ became involved, the NCA had worked with the social media provider to try to identify the users of the account. They had been able to narrow down the location of the account user to the Middle East, but could not positively identify the user or the country in which he was based. GCHQ analysis of communications data obtained through bulk interception warrants revealed that the user was based in Kuwait, identified him, and uncovered the fact that another person was also using the same account for the same purpose. The two individuals were subsequently arrested.

Without bulk interception, it would have taken months or years to identify the individuals and pass information to the Kuwaiti authorities. The most obvious alternatives, the use of data obtained from CSPs, has the disadvantages set out in Case Study 10 above.

Case study A8/12

GCHQ
Action
Cocaine trafficking

Between November 2014 and November 2015, GCHQ's analysis of data obtained under bulk interception warrants led to significant disruption of the cocaine trafficking trade from South America and the Caribbean to Europe. This involved the seizure of over 11 tonnes of cocaine, with an approximate street value of £1.1 billion. The nature of global communications and the communications methods of those involved in the international

drug trade mean that targeted interception is not a viable alternative; bulk interception is the only way in which the traffickers can be identified, tracked and disrupted.

Case study A8/13

GCHQ
Action
Human trafficking

In early 2015 GCHQ analysis of secondary data obtained under bulk interception warrants was able to identify the multiple communications methods used by the principal member of an organised crime group involved in human trafficking into the UK. GCHQ was also able to provide information on the individual's movements. This information enabled law enforcement officers to launch investigations which resulted in the release of a group of trafficked women from the control of the organised crime group. The individual was subsequently arrested and is awaiting trial.

ANNEX 9

CASE STUDIES – BULK ACQUISITION

CASE STUDIES
BULK ACQUISITION

Case study A9/1

MI5
Identify[269]
Counter-terrorism

In 2015, intelligence indicated that a number of individuals had travelled to Europe in order to conduct attacks in European capital cities. The names of the individuals were not known. MI5 was able to use bulk acquisition data to identify one individual who had travelled to the UK and then on to another European country. MI5 liaised with overseas intelligence agencies, and the information it provided assisted security agencies in locating the individual just two weeks after MI5 received the initial piece of intelligence.

Case study A9/2

MI5
Identify
Counter-terrorism: hoax threat

In this 2014 incident, a threat was made by telephone against an overseas embassy in London. The use of bulk acquisition data enabled MI5 swiftly to identify the user of the telephone as a known hoaxer. MI5 passed this information on to the police and embassy staff, so avoiding unnecessary and expensive police action and disruption to the work of the embassy.

Case study A9/3

MI5
Identify
Counter-terrorism

In 2015 MI5 analysis of bulk acquisition data identified a group of individuals in the UK with links to known extremists who aspired to conduct attacks. This analysis enabled MI5 quickly to focus investigative effort to mitigate the threat. MI5 worked with the police to disrupt the individuals concerned. Given the high threat posed by the links to the extremists, MI5 believes that without using bulk acquisition data it would not have been able to manage the risk so effectively.

[269] In each case study I have highlighted the nature of the principal work involved, by reference to the SIAs' Structured Description of Intelligence Work (Annex 4).

Case study A9/4

MI5
Identify
Counter-terrorism

In 2015 MI5 analysis of bulk acquisition data identified a previously unknown contact with a senior Islamist extremist. Given the significance of the contact, MI5 quickly deployed more intrusive, targeted resources. These techniques revealed to MI5 that the individual was aware of plans being developed to conduct attacks in the UK, and enabled MI5 to take steps to manage the threat. Without bulk acquisition data, MI5 is not confident that it could so quickly have identified the threat and managed the risk.

Case study A9/5

MI5
Identify
Counter-espionage

In 2015 the use of bulk acquisition data enabled MI5 to identify a national of a potentially hostile state who was suspected of being involved in espionage in the UK. The Review team was given information which indicated that, without bulk acquisition data, it is unlikely that the individual would have been identified.

The Review team was given details of MI5's counter-espionage operations: in a further example, analysis of bulk acquisition data alerted MI5 to the presence in the UK of another individual suspected of espionage. In this second case, MI5 worked with partners and took action to mitigate the threat. It had little time to take this action. Without the use of bulk acquisition data it might have been possible to detect the presence of the individual in the UK, but the necessary steps using targeted powers would have been significantly slower and in any event more intrusive.

Case study A9/6

MI5
Identify
Counter-terrorism

In 2013, intelligence indicated that an individual believed to be in contact with Islamist extremists had acquired a new phone. Acquiring the number of that phone was an MI5 investigative priority because of the risk that the individual would either carry out extremist activity himself, or provide assistance to other members of the group to which he belonged.

Information already in MI5's possession in relation to the individual's previous activity enabled it, using bulk acquisition data, to conduct analysis to identify the new phone. Once the phone had been identified, MI5 was able to obtain intelligence through more targeted analysis; this provided additional information about the individual's network and activities. The information led MI5 to conclude that, despite his contact with known extremists, this individual did not pose a threat in his own right. This conclusion enabled MI5 to release the resources that had been focused on the individual.

Without the availability of bulk acquisition data, MI5 would have had to undertake a significantly more time-consuming, costly and intrusive process, possibly including targeted communications data requests on the individual's associates, in order to identify the new phone. This approach would have required additional investigator resource to make the requests and analyse the results. MI5 also told the Review team that, pending identification of the new phone, expensive mobile surveillance of the individual would probably also have been deployed in order to mitigate the threat that this person was believed to present. Not only would this have been particularly intrusive, but the deployment of surveillance resources on this individual would inevitably have reduced MI5's capacity to obtain intelligence on other threats.

Case study A9/7

MI5
Identify
Counter-espionage

In 2014 MI5 learned that a British national, believed to be engaged in espionage in the UK for a potentially hostile state, had acquired a new mobile phone. MI5, using bulk acquisition data, was able to establish that the phone was likely to be one of a small number of candidate numbers. Further analysis of those phone numbers, involving the use of bulk acquisition data to identify and analyse the numbers called by each of those phones, enabled MI5 to identify the phone most likely to be used by the person in whom it was interested. Without the use of bulk acquisition data, targeted communications data would have been needed on each of the phones in order to identify the phone most likely to be used by the individual of interest. This form of targeting of a number of phones, all but one of which had innocent users, would have been far more intrusive and time consuming. Identifying the telephone of interest enhanced MI5's ability to identify activity of concern; the individual was assessed to present a risk, and steps taken to mitigate that risk.

Case study A9/8

MI5
Understand
Counter-terrorism

In late 2015 MI5 learned that a foreign national associated with ISIL had visited the UK for a period of time. Analysis of bulk acquisition data identified a previously unknown telephone used by the individual and enabled MI5 to learn more about his activity and contacts in the UK. This knowledge helped MI5 to understand the purpose of his travel and whether he had been involved in attack planning. MI5 was then able rapidly to re-focus investigative resource and to prioritise investigations. The Review team was shown material indicating that this work led to the disruption of activities of UK-based extremists. MI5 believes that without bulk acquisition data it is unlikely that the same result could have been achieved; if it could, it would certainly have taken longer. The individual in question is now awaiting trial in another country for terrorist offences.

Case study A9/9

MI5
Understand
Counter-terrorism

MI5 has used bulk acquisition data to understand more about Syria-linked attack planning in Europe and the UK. This work includes the analysis of bulk acquisition data to identify UK-based individuals with links to ISIL associates based overseas. MI5 has been able to use this information to manage the potential threats. The Review team was given details which indicated that without bulk acquisition data it would not have been possible to identify the individuals so quickly or with the same degree of certainty, and it would have taken vastly greater resources; it is likely that MI5 would have had to take a number of specialist data analysts and investigators away from other high priority work in order to deploy a range of targeted techniques. These specialists would then have had to analyse and assess the more fragmented intelligence which would probably have been obtained as a result.

Case study A9/10

MI5
Understand
Counter-terrorism
Summarised in the Operational Case

This case study related to the London and Glasgow attacks in 2007. Using bulk acquisition data, MI5 was able to establish within hours that the same perpetrators were responsible for both attacks. MI5 was also able, within a similarly short period, to learn more about the details of the attacks, including the methods used and the identities of those involved or associated with the attackers. The ability to conduct this analysis at pace enabled MI5 to support the police in responding swiftly to the attacks and to the threat of further, imminent attacks.

It would not have been possible to achieve the same results with comparable speed, using targeted queries. Speed was essential at the time, when the SIAs and police had to learn as quickly as possible whether other attacks were imminent. Bilal Abdulla was subsequently convicted of conspiracy to murder and conspiracy to cause explosions likely to endanger life. Kafeel Ahmed died of the injuries that he sustained at Glasgow Airport, having set himself alight.

Case study A9/11

MI5
Understand
Counter-terrorism
Summarised in the Operational Case

In 2010, a network of terrorists – comprising groups in Cardiff, London and Stoke-on-Trent - planned a series of bomb attacks at several symbolic locations in the UK, including the London Stock Exchange. Complex analysis of bulk acquisition data played a key role in identifying the network. The task was made particularly challenging by the geographical separation of the groups. Nine members of the network were subsequently charged and pleaded guilty to terrorism offences relating to the plot. Eight members of the network pleaded guilty to engaging in conduct in preparation for acts of terrorism.

MI5 reiterated to the Review team the assertion it had already made in public that the use of targeted communications data would not have allowed it to identify the attackers and understand the links between them with the speed made possible by the use of bulk acquisition data.

Case study A9/12

MI5
Understand/action
Counter-terrorism
Summarised in the Operational Case

Operation Overt was the 2006 MI5 and police investigation into a plot to mount multiple and simultaneous attacks on aircraft using home-made bombs. Had this plot succeeded, it would have been the largest ever terrorist attack launched from the UK, with a death toll comparable to that of 9/11. Bulk acquisition data enabled MI5 to identify the formerly unknown leader of a further cell in the UK. Without the use of bulk acquisition data, targeted techniques would have been required and would have resulted in the interference with the privacy of a large number of people, all but one of them of no intelligence interest.

Ten members of the network were subsequently convicted of offences relating to the plot.

Case study A9/13

MI5
Understand
Counter-terrorism

In this recent case, MI5 was aware that a number of individuals, believed to be involved in a plot to attack a UK target, were planning to travel overseas. Analysis of the group's communications activity and behaviour, including analysis of bulk acquisition data, was used to discover the date of the group's travel. Bulk acquisition was used in support of a wide range of investigative and operational techniques, and enabled MI5 to identify other individuals linked to the suspects. Two individuals were convicted of terrorism-related offences, and a further two were convicted of other offences.

Case study A9/14

MI5
Understand
Counter-terrorism

This case involved the monitoring of a group of extremists who were known to meet in a place used by other people of no intelligence interest. Analysis of bulk acquisition data helped to enable MI5 to establish when the group was going to meet. More intrusive

techniques were then put in place while the group was present; through these, MI5 obtained valuable intelligence on their connections to extremists overseas. Without bulk acquisition data, MI5 would have had to use more targeted measures, such as increased surveillance of members of the group. A further alternative would have been to monitor the meeting place. However, MI5 does not believe that the intelligence could have been obtained through these means without an unacceptable level of collateral intrusion, including the monitoring of people completely unconnected to the targets. The information obtained through bulk acquisition data contributed to the decision to ensure that measures were taken to prevent the individuals from travelling abroad.

Case study A9/15

MI5
Understand
Counter-terrorism

In 2015, MI5 was monitoring an individual who was known to be involved in attack planning in the UK, and whose mental health rendered him volatile and at risk of taking spontaneous action. Targeted intelligence revealed that the individual had obtained a new mobile phone. Bulk acquisition data was used to identify that phone, which was then subjected to targeted interception. The individual was arrested while committing a criminal offence, and was subsequently convicted.

Without bulk acquisition data, MI5 would have had to deploy more intrusive techniques in order to identify the phone. The alternative methods were explained to the Review team. All of these methods would have been more time-consuming, and some would have resulted in more collateral intrusion. They would also have been less efficient, and carried a greater risk of the correct phone not being identified. Further, had MI5 been unable to identify the phone and intercept communications, it would have had less certainty about the individual's plans and the risks that he posed. The police might have had to disrupt the individual's plans earlier than they did, in order to protect the public, and might have had to do so before obtaining evidence admissible in criminal proceedings.

Case study A9/16

MI5
Understand
Counter-terrorism

In 2015 MI5 was investigating an individual it believed might be likely to commit a spontaneous violent attack. The individual had potential access to firearms and MI5 believed that the person planned to travel to Syria and possibly aspired to conduct attacks in the UK. Intelligence indicated that the individual had a new telephone. Analysis of bulk acquisition data quickly identified that phone, which was then subjected to targeted interception. Following a joint MI5 and police operation, the individual's activities were disrupted.

Without bulk acquisition data, identifying the phone would have required more intrusive targeted techniques. All available methods would have been more time-consuming, and may have resulted in more collateral intrusion, while also offering less certain prospects of identifying the right phone. Further, had MI5 been unable to identify the phone and to intercept the individual's communications, it would have had less knowledge about the individual's plans and the risks that he posed. The police might have had to disrupt the individual's plans earlier than they did, causing important intelligence to be lost.

Case study A9/17

MI5
Action
Counter-terrorism

Bulk acquisition data was used in a recent operation to identify phones linked to a dissident republican attack in Northern Ireland. The information obtained, combined with other sources, led to the arrest and charge of an individual on terrorist offences. The telephones were not previously known to MI5. The Review team was given information which indicated that it would have taken more time and been considerably more resource intensive to discover the telephones without bulk acquisition data.

Case study A9/18

MI5
Bulk acquisition data and bulk personal datasets
Action
Counter-terrorism

Bulk acquisition data and BPD were used to discover that a UK national had returned to the UK, having attempted unsuccessfully to travel to Syria. Action was taken to disrupt his activities. MI5 believes that the individual has been successfully deterred from further attempts to travel to Syria.

Case study A9/19

MI5
Action/pattern analysis
Counter-terrorism
Summarised in the Operational Case

In 2007 bulk acquisition data was used to identify patterns of communication activity, leading to the identification of previously unknown telephone numbers used by a UK group of extremists planning to kidnap and murder a British Muslim soldier in the UK. They intended to film the soldier's death and send the film to their terrorist contacts abroad for public release. MI5's work enabled the police to search properties associated with the group, leading to the discovery of evidence of the plot which was admissible in court. Successful prosecutions followed.

The use of bulk acquisition data enabled MI5 to obtain information far more quickly than it could have done using targeted means.

Case study A9/20

MI5/police
Action
Counter-terrorism
Summarised in the Operational Case

In this 2009 case, MI5 was investigating intelligence of a specific UK attack plan. This intelligence was obtained through targeted means. However, it did not reveal the extent to which the plot had developed. Bulk acquisition data was used to establish that the threat to potential victims was not imminent. The knowledge obtained by MI5 from bulk acquisition data informed a joint police/MI5 decision to continue with evidence-gathering

for a prosecution (although the potential victims were warned and temporarily relocated). Without bulk acquisition data, uncertainty about the risk to the victims might have led the police to intervene sooner, without being able to gather the evidence needed for a prosecution. In fact, for reasons explained to the Review team, no prosecution followed.

Case study A9/21

MI5
Action
Counter-proliferation

MI5 used analysis of bulk acquisition data in order quickly to identify individuals in the UK linked to overseas weapons proliferation programmes. The Review team was shown material indicating that MI5 used this information to take action to mitigate the risks. Without the timely access to bulk acquisition data, MI5 believes that it would not have been able as effectively to disrupt this proliferation activity.

Case study A9/22

MI5
Action
Counter-espionage

Bulk acquisition data was used to identify contact between an intelligence officer of a potentially hostile state and a national of the same country in the UK. MI5 interviewed the UK-based individual, obtaining valuable information and disrupting any hostile work on the part of that person. MI5 told the Review team that, without the use of bulk acquisition data, it would have been difficult, if not impossible, for it to identify ongoing communications between the individuals; even if it were possible, far more intrusive techniques would have been required. The resulting interview would also have had less of an impact, because MI5 would have been unable to disclose details of information obtained through targeting without compromising intelligence sources. The interview would therefore have been unlikely to produce the intelligence that was in fact obtained.

Case study A9/23

MI5
Action
Counter-terrorism

Bulk acquisition data was used in 2014 to identify the mobile phone being used by a dissident Irish republican. The phone was then intercepted, and police were able to arrest the individual while he was committing a terrorism-related offence but before any harm had been caused. He was then prosecuted for a number of terrorism-related offences.

MI5 told the Review team that it would have been possible to identify the mobile phone without the use of bulk acquisition data. However, the alternative method would have involved significant collateral intrusion in the form of gathering information about many telephones, all but one of them of no intelligence interest. This method would also have taken longer, and so carried the risk that the correct phone might not have been identified in time to prevent an attack.

Case study A9/24

MI5
Action
Counter-terrorism

In 2014 bulk acquisition data were used by MI5 to identify telephones being used by dissident Irish republicans who were planning attacks. The phones were then intercepted. The knowledge gained from this operation informed the joint MI5 and PSNI investigative strategy. An individual was subsequently arrested and charged with terrorist and other offences.

Case study A9/25

MI5
Action
Counter-terrorism
Summarised in the Operational Case

In this 2013 case, bulk acquisition data was used to foil an attack by Irish dissident republicans. It was suspected that members of the group had already obtained explosives and that their activities were increasing (a common sign of an attack being imminent). However, MI5 did not know the date of any proposed attack and the group's security awareness made it difficult to obtain further information.

The use of bulk acquisition data identified telephones being used by the group, and further enabled MI5 to identify previously unknown members of the group. MI5 was able to increase its coverage of this expanded group. As a result it became aware of a sudden further increase in activity from analysis of the group's communications activity and MI5 judged that an attack was imminent. Police intervened and recovered an improvised explosive device. A prosecution followed.

The Review team was given details which indicated that, without bulk acquisition data, the telephones would not have been identified.

ANNEX 10

CASE STUDIES – BULK EI

CASE STUDIES
BULK EQUIPMENT INTERFERENCE

The SIAs have not yet undertaken any work involving the use of bulk equipment interference. GCHQ provided two case studies demonstrating the use of EI under the Intelligence Services Act; the equivalent use under the proposed legislation would be targeted thematic equipment interference. GCHQ explained that, in different circumstances, bulk equipment interference might be needed to achieve the same results.

The Operational Case included three hypothetical case studies, giving examples of situations in which the SIAs would wish to use bulk equipment interference. These case studies are set out below.

In addition, the Operational Case contained two hypothetical scenarios to demonstrate the difference between the circumstances in which targeted thematic EI would be appropriate, and bulk EI. These scenarios have been reproduced at the end of this Annex.

Case study A10/1

GCHQ
Bulk interception/targeted thematic EI
Identify/target discovery and development[270]
Counter-terrorism

Several hundred British extremists have travelled to Syria to join ISIL and many of these are actively involved in planning attacks against the UK and its allies. The UK cannot work co-operatively with the Syrian government to identify and disrupt these attack plans. In many cases it is extremely dangerous for a human source to go into ISIL territory.

This operation involved the identification of previously unknown Islamist extremists and also the identification of new phones or other devices used by known extremists who are based in Syria and who pose a threat to the UK and its international partners.

Intelligence from sources including bulk interception identified a location in Syria used by extremists. However the widespread use of anonymisation and encryption prevented GCHQ from identifying specific individuals and their communications through bulk interception. GCHQ then used EI under an ISA authorisation (under the Bill this would be

[270] In each case study I have highlighted the nature of the principal work involved, by reference to the SIAs' Structured Description of Intelligence Work (Annex 4).

done using a targeted thematic EI warrant) to identify the users of devices in this location.

From the data brought back, GCHQ was able to identify approximately 80 individuals for further investigation. Upon more investigation, it became apparent that some of these individuals were implicated in the highest priority threats to the UK and its international partners.

GCHQ gave the Review team examples of locations and intelligence requirements where this approach would be expected to deliver similar results but where the technological and physical environment meant that it would be necessary, in future, to conduct the operation under a bulk EI rather than targeted thematic EI warrant. In this specific case study, the only potentially viable option which might partially have replicated the results would have been the use of human sources to obtain information; even if this had been practicable, the risk to any human agent would have been very great, and the results less complete and less timely.

Case study A10/2

GCHQ
Identify/target development/action
Counter-terrorism

This case study related to part of an operation targeting extremists in Syria responsible for hostage-taking and attempted attacks on UK nationals. The location of the individuals and the technological environment in which they communicated made monitoring via bulk interception very challenging and inadequate.

In order to determine how these individuals were communicating, GCHQ conducted an EI operation against the wider area in which they operated under an ISA authorisation (under the Bill this would be done using a targeted thematic EI warrant). The operation identified the devices and individuals sought at the outset of the operation, and supported further intelligence work, both by GCHQ and its partners, against them.

Again the only potentially viable option which might partially have replicated the results obtained through EI would have been the use of human sources; again, the risks to any human agent would have been great, and the information would have taken longer to obtain and would have been less complete.

Case study A10/3

Hypothetical case study from the Operational Case
Protecting against a terrorist attack

A group of terrorists are at a training camp in a remote location overseas. The security and intelligence agencies have successfully deployed targeted EI against the devices the group are using and know that they are planning an attack on Western tourists in a major town in the same country, but not when the attack is planned for. One day, all of the existing devices suddenly stop being used. This is probably an indication that the group has acquired new devices and gone to the town to prepare for the attack. It is not known what devices the terrorists are now using. The security and intelligence agencies would use bulk EI techniques to acquire data from devices located in the town in order to try to identify the new devices that are being used by the group. If it is possible to identify those devices quickly enough, it may be possible to disrupt the attack. Without bulk EI powers, it is very unlikely that this would be achievable.

Case study A10/4

Hypothetical case study from the Operational Case
Countering biological weapons proliferation

A hypothetical totalitarian state has an indigenous email system which is mandated for use by the general population, but also by scientists working on the state's biological weapons programme who are involved in the proliferation of weapons technology. This means it is used by many thousands of people within that country. The security and intelligence agencies can only obtain limited data from interception which means it is not possible to identify particular accounts which belong to individuals of intelligence interest working on the biological weapons programme. Bulk EI techniques would be needed to access a limited amount of data relating to a very large number of users of the service – potentially even all its users. This would enable the security and intelligence agencies to filter out those who were associated with the biological weapons programme in order to use targeted EI techniques against them to support the UK's aim of disrupting their proliferation of biological weapons.

Case study A10/5

Hypothetical case study from the Operational Case
Cyber-defence

A state controlled agent provides the infrastructure to several other state controlled malicious Computer Network Exploitation (CNE) programmes. These programmes are responsible for espionage against the Government and UK industry at massive scale. The security and intelligence agencies' ultimate aim would be to identify that agent and any others supplying infrastructure to the programmes in order to find any of the new computer equipment before it is used.

In order to do this the security and intelligence agencies would need to use bulk EI to survey a location from where they believe the infrastructure is being procured, in order to identify activity characteristic of the procurers. In order to find these individuals, the security and intelligence agencies would need to acquire a large amount of data from which to identify likely candidates, who would then be subject to more targeted intelligence investigation.

Case study A10/6

Hypothetical examples from the Operational Case
The difference between targeted thematic and bulk EI

*Scenario: Intelligence suggests that a Daesh inspired cell in a particular location in the Middle East is plotting an imminent bomb attack against UK interests in the region. The intelligence requirement is for the security and intelligence agencies to find and identify all the individuals in the cell as fast as possible and uncover their plans. To do this, the communications of the individuals in the cell need to be acquired***.**

Example 1

Interception reveals that the cell are all using a unique anonymisation package to hide their online identities.

An EI warrant is used to obtain a high volume of equipment data (not content) from a large number of devices in the specified location in the Middle East. By applying a search term (a 'selector') that is unique to the anonymisation package to the 'pot' of data collected, only data relating to the cell members is retrieved for examination. From this information, the content from only the cell members' devices can then be collected and examined.

In this example, a specific identifier (the selector unique to the anonymisation package) which is connected directly to the cell members is known from the outset. Accordingly, despite the precise identities of the individuals being unknown, the Secretary of State:

- knows and can fully assess all of the interferences with privacy that will occur (both in relation to the cell members and innocent individuals whose devices will be affected) from the start to the end of the operation;

- knows what will happen at the beginning of the operation to collect the initial 'pot' of data; and

- knows, to a high degree of certainty given the specific identifier that will be applied to that 'pot', that the communications to be retrieved from the 'pot' and examined will belong to the cell members.

As the cell members can be identified from their association to a specific, known anonymisation package, a targeted 'thematic' warrant is suitable.

Example 2

By contrast with Example 1, little is known about the individual members of the terrorist cell. No technical details are known about their communications or the devices they are using. However, it is known that a particular software package is commonly – but not exclusively – used by some terrorist groups.

An EI warrant is used to obtain a large volume of equipment data (not content) from a large number of devices in the specified location in the Middle East. Using a specific search term (a 'selector') related to the software package, data relating to the users of the software package is retrieved from the 'pot' of data collected.

Analysts apply other search terms and analytical techniques to the data to find common factors that indicate a terrorist connection. The results show that some people from the original 'pot' (those using the software package associated with terrorists) have also accessed a particular Internet Protocol (IP) address which is known to be linked to an extremist website containing, among other things, a bomb-making manual. Using the newly discovered IP address, the original 'pot' of data is searched again to find other devices that have also accessed the website. A series of refined searches of this kind will gradually identify devices that belong to the terrorist cell. Their communications (including content) can then be collected and examined.

By contrast with Example 1, no identifiers which relate solely to the targeted individuals are known from the outset. The only identifier known at the outset is the software package used by terrorists but also by some other, innocent individuals. The IP address linked to the extremist website and the other refining factors were only uncovered during the course of the operation through analysis of the original 'pot' of data.

Consequently, the Secretary of State cannot know or fully assess all of the interferences with privacy that will occur (both in relation to the cell members and innocent individuals whose devices will be affected) from the start to the end of the operation. The Secretary of State knows:

- the objective and the scale of the operation and what will be done in order to collect the initial 'pot' of data;

- that the information to be retrieved from the 'pot' of data will likely include the data of terrorists, that will lead to the cell, but also some data belonging to innocent individuals (given the software package is not exclusively used by terrorists); and

- that further analytic work will be required leading to more refined searches on the initial 'pot' in order finally to discover and obtain the communications of the terrorist cell.

But at the point of issuing the warrant, the Secretary of State is not in a position to assess the necessity and proportionality of subsequent searches of the 'pot'. To ensure that all of those searches are carried out in accordance with privacy considerations, additional examination safeguards need to be in place.

As the cell members can only be identified following considerable target discovery effort, a bulk EI warrant is suitable.

ANNEX 11

CASE STUDIES - BPD

CASE STUDIES
BULK PERSONAL DATASETS

Case study A11/1

MI6
Identify/target development[271]
Agent recruitment

Over a number of months in early 2016, the use of BPDs enabled MI6 to identify the travel to the UK of individuals of intelligence interest to the SIAs. The Review team was given information which demonstrated that, without the use of BPDs, the identification of these individuals would not have been possible. During the course of this year, six of these individuals have been identified as potential agents and been the subject of MI6 operational activity.

Case study A11/2

MI6
Identify/anomaly detection/pattern analysis
Counter-espionage

In late 2015, BPDs were used to analyse patterns of behaviour from which potential hostile actors could be identified. Cathryn McGahey QC was shown the report of the data scientists who conducted the analysis. The Review team was given details which demonstrated that (i) without the use of BPDs, such identification would not be possible; and (ii) the information gleaned was of significant use to the UK.

Case study A11/3

MI6
Identify
Counter-espionage

In 2013, BPDs were used to identify employees of an intelligence service potentially hostile to the UK. The Review team was given information which demonstrated that these identifications could not have made without the use of BPDs. The information was shared with intelligence partners.

[271] In each case study I have highlighted the nature of the principal work involved, by reference to the SIAs' Structured Description of Intelligence Work (Annex 4).

Case study A11/4

MI6
Identify
Counter-proliferation

This study, from early 2015, involved the use of BPDs to identify an individual who could be approached to report on the weapons capability of a potentially hostile state. Cathryn McGahey QC was shown contemporaneous documents which showed that the approach was successful and which included examples of the reports provided to MI6 by that individual. The Review team was given details which demonstrated that (i) no reasonable alternative to the use of BPDs could have been used to identify the pool from which a small number of eligible individuals were eventually selected; and (ii) the objective was one of substantial importance to the UK.

Case study A11/5

MI6, MI5 and GCHQ
Identify/target discovery and development
Counter-terrorism

In mid-2016, following attacks in Paris and Brussels, MI6 worked in partnership with MI5 and GCHQ to identify individuals in ISIL networks who posed a threat to the UK. MI6 used BPDs to identify a number of such individuals. Without the use of BPDs, it would not have been possible to identify these individuals. Following this work, the SIAs were able to take steps to reduce the threat that they posed to the UK.

Case study A11/6

MI6
Identify/target discovery
Counter-terrorism

Since 2014, MI6 has been tasked with collecting intelligence on the membership of ISIL. In early 2016, the media reported the existence of approximately 20,000 leaked ISIL registration papers. However, in most cases the information in the documents was not of sufficient quality to enable the SIAs to make a positive identification, with high confidence, of members of ISIL who might pose a threat to the UK. It was only when this information was combined with information obtained from BPDs that MI6 was able positively to identify a number of individuals on the list who posed a threat to national security.

Case Study A11/7

MI6
Identify/target discovery
Agent recruitment
Summarised in the Operational Case

The SIAs were tasked by the Joint Intelligence Committee to produce intelligence on a country which threatened the UK's national security. MI6 was able to identify an individual who might provide useful intelligence but needed a way to make contact with that individual. A direct approach might have placed that person at risk from his country's own internal security service**.** Through the use of BPDs, MI6 was able to identify a third person who could more safely make contact with the target individual. That third person has successfully been recruited as an agent.

Case study A11/8

MI5
Identify/target discovery
Counter-terrorism

This case dated from 2004-5. MI5 sought to identify a member of Al Qaeda who was believed to be a potential suicide operative in the UK. MI5 knew that he was British and knew his approximate age; it also had some information relating to his previous travel. The use of BPDs enabled the pool of potential candidates to be narrowed from 27,000 (based on the travel information), to 3,000 (using biographical and travel information BPDs), then to 40 (using further travel information BPDs) and finally to one (using passport data). Following extensive work by other methods to corroborate the belief that the individual selected through BPDs was a potential suicide operative, MI5, working with intelligence partners, disrupted this person's activities. It believes that he subsequently disengaged from Islamist extremism.

Case study A11/9

MI5/law enforcement agency
Identify/target discovery/action
Counter-terrorism
Summarised in the Operational Case

MI5 learned that an individual, in contact with a known extremist, was planning to travel to Syria imminently. MI5 only had partial identifying details for the prospective traveller. Analysis of the known extremist's communications provided hundreds of contacts, any one of which could have been the person of interest. Through the use of bulk BPDs, within one day those hundreds were reduced to one candidate who matched the known

details. This enabled MI5 to work with law enforcement colleagues to build a strategy to prevent any attempted travel and rapidly to focus investigative effort to build coverage of activities of national security concern.

Without access to BPDs, MI5 might have tried to identify fully each of the hundreds of contacts of the known extremist. However, this approach would have involved intrusion into hundreds of individuals of no intelligence interest, and might not have identified the individual prior to travel. A further alternative, that of interception of the known extremist's phone, would equally have been more intrusive, might have taken more time (including the time needed to obtain a warrant) than MI5 believed to be available, and would not necessarily have identified the traveller.

Case study A11/10

MI5
BPDs and bulk acquisition data
Identify
Counter-terrorism
Summarised in the Operational Case

In 2014 MI5 received intelligence that an unnamed member of Al Qaeda was suspected of facilitating suicide bombers in the UK. The intelligence contained only one identifier for the person (but not a name). Using BPDs, a strong candidate for the individual was identified. During the course of this analysis, less intrusive means of identifying the individual were explored but these did not assist in identification. At this point, more intrusive techniques were deployed to provide positive confirmation of identity. These techniques led MI5 to conclude that the individual did not in fact pose a threat to national security. MI5 was then able to re-focus scarce resources towards other targets.

Case study A11/11

MI5
Identify
Counter-terrorism
Summarised in the Operational Case

During the 2012 London Olympics, interrogation of bulk personal data was used to establish whether any of the individuals who might have had access to venues had links with subjects of intelligence interest, and therefore might pose a threat. MI5 identified a number of such individuals who could potentially have posed a threat, and was able to take action further to investigate and manage the risk. The Review team saw material which showed that analysis of BPDs enabled MI5 rapidly to assess and rule out individuals initially thought to pose a potential threat, enabling it to focus more intrusive resources on the individuals of greatest concern. Access to BPDs enabled MI5 to draw

links between individuals far more easily and quickly than it would have been able otherwise to do, and to ensure that it focused resources where most appropriate.

Case study A11/12

MI5
Identify/target development/action
Counter-terrorism
Summarised in the Operational Case

MI5's holding of BPDs includes lists which identify individuals in the UK likely to have access to firearms. These BPDs are checked against the names of known terrorists and as part of specific investigations. The information is believed by MI5 to have particular value, since recent overseas attacks, including the Paris attacks, have involved the use of firearms.

Case study A11/13

MI5
Action
Counter-terrorism

BPDs were analysed in 2015 by MI5, with advice from the Joint Terrorism Analysis Centre, to identify likely locations for entry to the UK being used by Islamic extremists. This information enabled counter-terrorism resources to be prioritised. This exercise has been found to be of value and will be updated.

Case study A11/14

MI5
Action
Counter-terrorism
Summarised in the Operational Case

In this case, MI5 had obtained intelligence to indicate that a number of Islamist extremists were planning to travel to the UK in order to carry out an attack. The use of BPDs suggested that one individual was travelling to the UK earlier than had been expected. This knowledge enabled resources to be concentrated on this person, and led to him being stopped on his arrival in the UK and valuable intelligence obtained. Without the use of BPDs, MI5 would not have had the advance notice necessary to stop the individual.

Case study A11/15

MI5
Action
Counter-terrorism
Summarised in the Operational Case

In this case, BPDs were used to identify a person said to be in possession of a firearm used in an attack in the UK, and also to identify the address at which the weapon was said to be located. Other intelligence confirmed the location of the weapon, which was retrieved. Prosecution followed.

ISBN 978-1-4741-3691-4