Report of the Interception of Communications

Report of the Interception of Communications Commissioner

July 2016

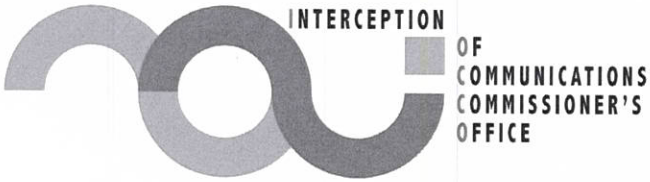
Review of directions given under section 94 of the Telecommunications Act 1984

Presented to Parliament pursuant to Section 58(6) of the Regulation of Investigatory Powers Act 2000

Ordered by the House of Commons to be printed on 7th July 2016

Laid before the Scottish Parliament by the Scottish Ministers on 7th July 2016

HC 33
SG/2016/67



© Crown copyright 2016

This publication is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated. To view this licence, visit nationalarchives.gov.uk/doc/open-government-licence/version/3 or write to the Information Policy Team, The National Archives, Kew, London TW9 4DU, or email: psi@nationalarchives.gsi.gov.uk.

Where we have identified any third party copyright information you will need to obtain permission from the copyright holders concerned.

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

Any enquiries regarding this publication should be sent to: info@iocco-uk.info

You can download this publication from www.iocco-uk.info

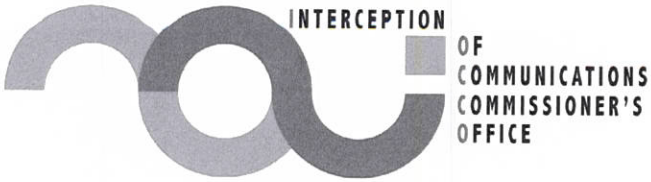
Printed in the UK by the Williams Lea Group on behalf of the Controller of Her Majesty's Stationery Office

Print ISBN 9781474133654

Web ISBN 9781474133661

ID 26051603 06/16

Printed on paper containing 75% recycled fibre content minimum



The Rt Hon. David Cameron MP
Prime Minister
10 Downing Street
London
SW1A 2AA

June 2016

Dear Prime Minister,

You appointed me under section 57(1) of the Regulation of Investigatory Powers Act (RIPA) 2000 as Interception of Communications Commissioner to take office from 4th November

Our review and this report highlight clearly the difficulties when statutes are operated in secret and where there is a lack of statutory codified procedures. We have made extensive recommendations throughout this report which the relevant intelligence and law enforcement agencies should introduce to clarify and bring consistency to the procedures in place, remedy the lack of record-keeping requirements and ensure that we are able to undertake our oversight of the giving and use of section 94 directions properly. I require the agencies and the public electronic communications networks (PECNs) to implement the recommendations without delay.

You are required to lay a copy of my half-yearly reports before each House of Parliament (together with a statement as to whether any matter has been excluded because it has appeared to you, after consulting me, that publication of that matter would be contrary to the public interest or prejudicial to matters specified in section 58(7) of RIPA). My expectation is that you will feel able to lay this entire report before Parliament.

I am well into the process of completing my second half-yearly report which covers the work undertaken by my office in the calendar year of 2015 and my intention is to submit that report to you before the summer recess.

Yours sincerely,

The Rt Hon. Sir Stanley Burnton
Interception of Communications Commissioner

Contents

Section 1	The role of the Interception of Communications Commissioner	2
Section 2	Background and purpose of the review of section 94 directions	3
Section 3	Investigatory Powers Tribunal (IPT) case - IPT/15/110/CH	7
Section 4	The Telecommunications Act 1984	9
Section 5	Requirement for information for the IOCCO review	14
Section 6	Inspection of the documentation and information provided to the review	17
Section 7	Statistical information for section 94 directions	20
Section 8	Review of section 94 directions to acquire bulk communications data	21
Section 9	Review of "other" section 94 directions	44
Section 10	The Investigatory Powers Bill ("IP Bill")	49
Section 11	Summary and conclusions	51
Section 12	Recommendations	54

Section 1

The Role of the Interception of Communications Commissioner

1.1 The Interception of Communications Commissioner ("the Commissioner") is appointed by the Prime Minister under section 57(1) of the Regulation of Investigatory Powers Act (RIPA) 2000 to keep under review, amongst other things, the interception of communications and the acquisition and disclosure of communications data under of Part 1 of RIPA. The Commissioner is required to make half-yearly reports to the Prime Minister with respect to the carrying out of his functions.

1.2 As indicated in our March 2015 report[2] the Prime Minister asked the then Commissioner, the Rt Hon. Sir Anthony May, to formally oversee directions issued under section 94 of the Telecommunications Act 1984 (hereafter "section 94 directions"). Our oversight of section 94 directions is currently on a non-statutory basis. The Investigatory Powers Bill, currently being considered by Parliament, includes provisions to address this.

[2] See Section 10 (page 78) http://www.iocco-uk.info/docs/IOCCO%20Report%20March%202015%20(Web).pdf

Section 2

Background and purpose of the review of section 94 directions

Background

2.1 The Prime Minster wrote to the former Commissioner in January 2015 to ask him to extend his oversight to include directions given by a Secretary of State under section 94 of the Telecommunications Act 1984. It was acknowledged that the Commissioner had previously provided *limited* non-statutory oversight of the use made of one particular set of directions by the Security Service. The Prime Minister was keen to extend that oversight.

2.2 The Commissioner responded that month agreeing to his role being extended and asked for clarification on the mechanism and authority under which the oversight would take effect. The Commissioner also highlighted a number of important points of detail that required careful consideration:-

- IOCCO had been working to improve the transparency of, and public confidence in, the oversight undertaken more generally. The Commissioner had expressed concerns to the Home Secretary previously about his inability to discuss publicly his *limited* oversight of one particular set of section 94 directions.
- For this reason the Commissioner's preference was for him to avow this oversight in his next half-yearly report (subsequently published in March 2015[3]).
- Clarification was required as to whether his function would include oversight of the necessity and proportionality of any section 94 directions; oversight of the use of the directions; oversight of the access to the material obtained pursuant to any direction (where relevant); and, oversight of the retention, storage and destruction arrangements for any material obtained (where relevant); and

[3] See Section 10 of March 2015 Report http://www.iocco-uk.info/docs/IOCCO%20Report%20March%202015%20(Web).pdf

- A review would need to be conducted to scope the oversight, and there would be a requirement for additional staff (and possibly technical facilities) to ensure the additional oversight was carried out effectively.

2.3 The Prime Minister responded to the Commissioner in February 2015 clarifying that:-

- There was no mechanism short of legislation to put the oversight of section 94 directions on a statutory footing. The oversight, would, therefore have to be on a non-statutory basis in the short term, but he hoped it was something that could be addressed in the next Parliament.
- The oversight would include all of the areas outlined by the Commissioner.

Avowal of the use of section 94 directions to acquire bulk communications data

2.4 On the 4th November 2015 the Home Secretary (The Rt Hon. Theresa May MP) made a statement in the House of Commons[4] about the draft Investigatory Powers Bill, a proposed new law consolidating and updating investigatory powers, strengthening safeguards, and establishing a revised oversight regime:

> *"I have announced today our intention to ensure that the powers available to law enforcement and the agencies are clear for everyone to understand. [...] There remain, however, some powers that successive Governments have considered too sensitive to disclose, for fear of revealing capabilities to those who mean us harm. I am clear that we must now reconcile that with our ambition to deliver greater openness and transparency."*
>
> *"The Bill will make explicit provision for all of the powers available to the security and intelligence agencies to acquire data in bulk. That will include not only bulk interception provided under the Regulation of Investigatory Powers Act 2000 and which is vital to the work of GCHQ, but the <u>acquisition of bulk communications data</u>, both relating to the UK and overseas."* [emphasis added]

[4] See Hansard - 4 Nov 2015: Column 971

"That is not a new power. It will replace the power under Section 94 of the Telecommunications Act 1984, under which successive Governments have approved the security and intelligence agencies' access to such communications data from communication service providers."

Scope of oversight function

2.5 The Commissioner's oversight function is to include oversight of:

(i) Section 94 directions to acquire *bulk communications data.* See **Section 8** of this report for our review of section 94 directions to acquire bulk communications data which included:

- a number of section 94 directions given on behalf of the Security Service which were previously overseen on a *limited* basis by the Interception of Communications Commissioner. This previous oversight (between 2006 and 2015) was *limited* because it was only concerned with the authorisations to access the communications data obtained pursuant to the directions. The oversight was not concerned with, for example, the giving of the section 94 directions by the Secretary of State (including the necessity and proportionality judgements by the agency or Secretary of State) or the arrangements for the retention, storage and destruction of the data. In 2015 this oversight was transferred to IOCCO, at the request of the former Commissioner the Rt Hon. Sir Anthony May, and since then it has taken place at the same time as the Security Service's annual communications data inspection under Chapter 2 of Part 1 of RIPA.;
- a number of section 94 directions given on behalf of GCHQ which were overseen by the Intelligence Services Commissioner[5] between 2006 and 2015. Prior to that they were overseen by a previous Interception of Communications Commissioner (between 2004 and 2006).

(ii) "Other" section 94 directions (i.e. not for bulk communications data) given on behalf of the intelligence agencies ("the agencies") or other public authorities (such as the Metropolitan Police Service Counter Terrorism Command (MPS CTC)) which were not overseen previously by any Commissioner. These include directions given,

[5] http://intelligencecommissioner.com/default.asp

for example, for the provision of services in emergencies, for civil contingency purposes or to help the agencies in safeguarding the security of their personnel and operations. **Section 9** of this report sets out our review of those directions.

2.6 The Prime Minister stated in his letter to the Commissioner that our oversight of section 94 directions would *not* extend to any section 94 directions given to public electronic communications networks (PECNs) which relate to the work of the Office of Communications (Ofcom), for example, those which we understand to have been given as part of market regulation or to establish the minimum security requirements of networks.

2.7 The Prime Minister also stated in his letter to the Commissioner that our oversight of section 94 directions would *not presently* extend to any section 94 directions given on behalf of the Department for Business, Innovation and Skills (BIS) because they were in the process of being reviewed and would possibly be rescinded. It has not yet been confirmed to us whether the Cabinet Office review has completed and what the status of these directions is.

Purpose of the review

2.8 This review started in October 2015, after IOCCO had secured the additional staffing resource. The purposes of this review were:

- to identify the extent to which the agencies and other public authorities use section 94 directions, in other words what has been done and by whom and for what purpose;
- 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.

Section 3

Investigatory Powers Tribunal (IPT) case - IPT/15/110/CH

3.1 It is useful to set out our function and how it differs from the role of the Investigatory Powers Tribunal[6] (IPT) as prescribed by section 65 of the Regulation of Investigatory Powers Act (RIPA) 2000. The IPT has an exclusive role in the United Kingdom in proceedings for actions that are incompatible with the European Convention on Human Rights (ECHR) and to consider and determine complaints made relating to conduct (or proposed conduct) by or on behalf of the agencies or complaints where a person believes they are aggrieved by conduct under RIPA. We are an expert review body and our role is to independently audit the relevant public authorities' compliance against *existing* legislation.

3.2 Whilst undertaking our review of section 94 directions we have had to be mindful of a case, Privacy International v. Secretary of State for Foreign & Commonwealth Affairs et al., currently before the Investigatory Powers Tribunal (IPT), which is relevant to section 94 directions for bulk communications data and other matters (i.e. bulk personal datasets).

3.3 Our review of section 94 directions did not seek to determine whether the section 94 regime is sufficiently clear and accessible to satisfy the requirements of English law, including those in the European Convention on Human Rights (ECHR), incorporated into English law by the Human Rights Act, as this is the exclusive role of the IPT, which it will address in the case referred to in the preceding paragraph. In this report, therefore, we have assumed that these requirements are satisfied, but we should not be taken as expressing any view on this.

3.4 Our review seeks to provide a factual account of how section 94 of the Telecommunications Act 1984 has been used by public authorities, to give an overview of the systems and procedures in place and to highlight any compliance issues.

[6] http://www.ipt-uk.com/

3.5 Whilst carrying out our review we have had to take account of the ongoing IPT case for two reasons. First, a significant amount of material relevant to this review has been disclosed to Privacy International, which we have had to consider carefully. Secondly, the IPT has given guidance to the respondents (the agencies) as to what material may be withheld from open proceedings on national security grounds. In the light of this we sought guidance from the IPT as the Commissioner would not, in general, wish to disclose material that the IPT has decided should remain in the closed proceedings for reasons of national security. This does not however prevent the Commissioner from determining at a later date that it might be in the public interest or might not be prejudicial to national security for further material to be published.

3.6 A significant number of the documents that have been disclosed in open have already been made available publicly by Privacy International[7]. We did not see the value in repeating large amounts of information already contained in these documents which are in the public domain.

3.7 The IPT has, pursuant to section 57(3) of RIPA, required assistance from the Commissioner in connection with the Privacy International case. That assistance is distinct from this review.

[7] https://www.privacyinternational.org/legal-actions

Section 4

The Telecommunications Act 1984

Background

4.1 The backdrop to the Telecommunications Act 1984 was the privatisation of British Telecom and the deregulation of the telecoms market within the United Kingdom.

4.2 The main provisions of the Telecommunications Act 1984 included:

- Privatising British Telecom;
- Establishing the Office of Telecommunications (now Ofcom) as a regulator to protect consumers' interests and market competition;
- Setting standards for modems according to the British Approvals Board for Telecommunications rules;
- Creating a criminal offence concerning indecent, offensive or threatening phone calls.

Public electronic communications network (PECN)

4.3 A public electronic communications network (PECN) is defined in section 151 of the Communications Act (2003) as:

> *"an electronic communications network provided wholly or mainly for the purpose of making electronic communications services available to members of the public."*

4.4 The term PECN excludes those who provide services or networks that are not available to members of the public (typically, private networks and the services run on private networks, and other bespoke services) [8].

[8] See "What kind of network or service are you providing?" at http://stakeholders.ofcom.org.uk/telecoms/ga-scheme/general-conditions/general-conditions-guidelines/

Section 94 directions

4.5 The Communications Act 2003 made amendments [shown in square brackets] to the Telecommunications Act 1984 some 19 years after its implementation.

4.6 Section 94 of the Telecommunications Act 1984[9] provides that any Secretary of State may, after consultation with a PECN to whom the section applies, give to that PECN 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:

> *S.94 (1) The Secretary of State may, after consultation with a person to whom this section applies, give to that person such directions of a general character as appear to the Secretary of State to be* ***[****necessary*[10]***]*** *in the interests of national security or relations with the government of a country or territory outside the United Kingdom.*

4.7 A section 94 direction may require (according to the circumstances of the case) the PECN to do, or not do, a particular thing specified in the direction:

> *S.94 (2) If it appears to the Secretary of State to be* ***[****necessary*[11]***]*** *to do so in the interests of national security or relations with the government of a country or territory outside the United Kingdom, he may, after consultation with a person to whom this section applies, give to that person a direction requiring him (according to the circumstances of the case) to do, or not to do, a particular thing specified in the direction.*

4.8 The power given to any Secretary of State to give directions under section 94 of the Telecommunications Act 1984 is therefore very broad.

4.9 The Secretary of State is not to give a section 94 direction unless he or she believes that the conduct required by the direction is proportionate to what is sought to be achieved by that conduct:

---

[9] http://www.legislation.gov.uk/ukpga/1984/12/section/94

[10] Words in s. 94(1) substituted (25.7.2003 for specified purposes and 18.9.2003 otherwise) by Communications Act 2003, (c. 21), ss. 406, 408, 411, {Sch. 17 para. 70(2)} (with Sch. 18); S.I. 2003/1900, arts. 1(2), 2, 3(1), Sch. 1, Sch. 2 (with art. 3(2) (as amended (8.12.2003) by S.I 2003/3142, art. 1(3)). The words replaced were "requisite or expedient".

[11] Words in s. 94(2) substituted (25.7.2003 for specified purposes and 18.9.2003 otherwise) by Communications Act 2003, (c. 21), ss. 406, 408, 411, {Sch. 17 para. 70(3)} (with Sch. 18); S.I. 2003/1900, arts. 1(2), **2**, 3(1), Sch. 1, Sch. 2 (with art. 3(2) (as amended (8.12.2003) by S.I. 2003/3142, art. 1(3)).

S.94 [(2A) The Secretary of State shall not give a direction under subsection (1) or (2) unless he believes that the conduct required by the direction is proportionate to what is sought to be achieved by that conduct.[12]*]*

4.10 Although there must have been consultation with the PECN prior to the direction being given, there is no requirement for the PECN to agree to the direction and, once the section 94 direction has been given, the PECN must comply with the direction.

4.11 Section 94(4) provides that the Secretary of State shall lay before each House of Parliament a copy of every direction given under this section unless he is of opinion that disclosure of the direction is against the interests of national security or relations with the government of a country or territory outside the United Kingdom, or the commercial interests of any person.

4.12 Section 94(5) provides that a person shall not disclose, or be required by virtue of any enactment or otherwise to disclose, anything done by virtue of this section if the Secretary of State has notified him that he or she is of the opinion that disclosure of that thing is against the interests of national security or relations with the government of a country or territory outside the United Kingdom, or the commercial interests of some other person.

4.13 Section 94(6) provides that the Secretary of State may, with the approval of the Treasury, make grants to PECNs for the purpose of defraying or contributing towards any losses they may sustain by reason of compliance with the directions given under this section. Section 94(7) provides that there shall be paid out of money provided by Parliament any sums required by the Secretary of State for making grants under this section.

Codes of practice, policies and procedures for the operation of section 94 of the Telecommunications Act 1984

4.14 Section 94 of the Telecommunications Act 1984 authorises the Secretary of State to give a direction of a "general character" to a PECN. There is no provision for the Secretary of

[12] S. 94(2A) inserted (25.7.2003 for specified purposes and 18.9.2003 otherwise) by Communications Act 2003, (c. 21), ss. 406, 408, 411, {Sch. 17 para. 70(4)} (with Sch. 18); S.I. 2003/1900, arts. 1(2), **2**, 3(1), Sch. 1, Sch. 2 (with art. 3(2) (as amended (8.12.2003) by S.I. 2003/3142, art. 1(3))

State to issue any codes of practice relating to the exercise or performance and duties under section 94 directions. Such a code of practice would include, for example:

- what should be in an application to a Secretary of State for a section 94 direction, including guidance in relation to necessity and proportionality;
- the duration for which a section 94 direction can be given;
- procedures specifying how a direction is to be reviewed, renewed, modified or cancelled (and by whom);
- where a direction relates to the acquisition of bulk communications data the processes and considerations concerning the retention and destruction of the data;
- where a direction relates to the acquisition of bulk communications data, the processes and considerations as to when, how, for what purpose and by whom the data retained may be accessed by a member of a public authority; and,
- matters relating to what constitutes an "error" in the giving of a direction, any conduct undertaken to comply with the direction, or in the subsequent access to data obtained under a direction, and the process for the reporting of errors.

4.15 Furthermore, the Telecommunications Act 1984 does not contain any specific requirements concerning the format and content of a section 94 direction. For example, there is no requirement for a section 94 direction:

- to be given in writing or in a manner that produces a record of it having been given;
- to describe the specific conduct to be undertaken by the PECN, for example, where the section 94 direction is for bulk communications data, what communications data is to be obtained or disclosed;
- to specify the statutory necessity purpose for which it was given, i.e. in the interests of national security;
- to specify the name of the Secretary of State giving it and the date it is given and will expire; or
- to specify the manner in which any disclosure is to be made or any conduct required is to be undertaken by the PECN.

4.16 In practice, in the absence of any codified procedures in or under section 94 of the Telecommunications Act 1984, the public authorities have developed processes to facilitate applying to a Secretary of State for a section 94 direction and to review, modify and cancel section 94 directions.

4.17 Where the section 94 directions relate to the acquisition of bulk communications data the procedures to be followed have been set out publicly in handling arrangements[13] published by the agencies in November 2015. Where the section 94 directions do not relate to the acquisition of bulk communications data there are no published arrangements concerning the processes to be followed.

13 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473780/Handling_arrangements_for_Bulk_Communications_Data.pdf

Section 5

Requirement for information for the IOCCO review

5.1 This review is wholly different from our oversight of Part 1 of RIPA (the interception of communications and the acquisition and disclosure of communications data). Section 58(1) of RIPA imposes an obligation on everyone concerned in the process to disclose all such documents or information as we may require to carry out our oversight, and there are detailed procedures and stringent record-keeping requirements set out in the Codes of Practice accompanying RIPA.

5.2 Section 94 of the Telecommunications Act includes no provision for independent oversight. Nonetheless, when carrying out this review, we received full cooperation from staff within the relevant public authorities and the PECNs.

5.3 In our July 2015 report[14] we set out a number of challenges presented by this review which stemmed from the facts that:

- the directions are **secret** as allowed for by statute[15];
- they can be given by *any* Secretary of State;
- they do not automatically expire after a defined period; and
- there was not, at the time of the July 2015 report, any comprehensive central record of the section 94 directions that had been given by the various Secretaries of State.

5.4 We have already mentioned in section 3 of this report a number of challenges associated with the ongoing IPT case. In addition, there is no code of practice or any written requirement for detailed record-keeping for public authorities or PECN's applicable to the operation of section 94 of the Telecommunications Act 1984.

[14] See Section 4 (pages 13-14) http://www.iocco-uk.info/docs/2015%20Half-yearly%20report%20(web%20version).pdf
[15] See paragraphs 4.37 and 4.38 of this report

Section 6

Inspection of the documentation and information provided to the review

PECNs

6.5 Our liaison with and visits to all the PECNs who hold section 94 directions included discussions with Chief Executives, heads of legal services, managers dealing with legal compliance and technical experts. Our liaison with the PECNs greatly assisted us to develop some areas to explore further when engaging with the public authorities.

6.6 During these visits we sought to gain an understanding of:

- what consultation took place with the PECN before the section 94 direction was given by the Secretary of State and who undertook the consultation;
- whether the section 94 directions made explicit what conduct the PECN was being directed to undertake. For example, where the direction was for bulk communications data, what data the PECN was being required to provide or disclose;
- whether there was a need for further discussion, clarification or review and if so how that was undertaken;
- the systems and procedures in place to operate the direction (for example arrangements concerning physical security, audits, retention etc.).

6.7 We confirmed that, in accordance with section 94(1) of the Telecommunications Act 1984, extensive engagement and consultation by the public authorities had been undertaken with the PECNs in all cases prior to the section 94 directions being given. All of the PECNs reported that the engagement and consultation had been, and remain, a key element for them especially when a legal advisor from the public authority has been available to discuss key aspects of what was being proposed. However some of the PECNs did raise some general areas of concern, for example:

- concerns relating to reputational (and commercial) risks to the PECN as the way the law is presented it may be inferred the PECN had agreed to the section 94 direction being given when that was never the case;
- that the section 94 provisions do not consider the multi-national nature of the PECN's business model or the fact that they have to operate in several legal jurisdictions;
- some PECNs could not, because of the security classification of the section 94 directions, retain a copy of the legal document on their premises and relied on the public authority retaining it on their behalf;

- concerns as to whether the bulk communications data they had disclosed had been shared with agencies in other jurisdictions. In one case a PECN had asked the agency to ensure that this did not happen and we were able to confirm that their data had not been shared with another jurisdiction. In other cases PECNs stated they would be very concerned if their data was shared with other jurisdictions without their knowledge. Of course information which is derived from the analysis of bulk communications data may form the basis of an intelligence report which is shared with another jurisdiction. The agencies have procedures governing the disclosure of communications data which are set out in the published handling arrangements[16].
- concerns about the cost to the PECN to set up or support the conduct required to be undertaken by the direction. On this point sections 94(6) and (7) of the Telecommunications Act 1984 permit the Secretary of State to make grants to PECNs for the purpose of defraying or contributing towards any losses they may sustain by reason of compliance with the directions given.

6.8 It became evident to us that in practice there is an ongoing strategic relationship between the public authorities' relationship teams and the PECN, commencing with an extended consultation before the direction is given, involving the determination of what is feasible or practicable, the costs involved, the security arrangements for the secure electronic transfer of the data (where relevant) and so on. There was evidence of continuing engagement between the relevant public authority to support the work of the PECNs, providing advice on legal and technical issues so that the PECNs were better able to comply with the section 94 directions.

6.9 We have already made clear earlier in this report that although there is consultation with the PECN prior to the direction being given, there is no requirement for the PECN to agree to the direction, and once the direction has been given they are under an obligation to comply with it. In all cases the Secretary of State had notified the PECN that he or she was of the opinion that the disclosure of anything done by virtue of the section 94 direction would be against the interests of national security.

16 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473780/Handling_arrangements_for_Bulk_Communications_Data.pdf

Section 7

Statistical information for section 94 directions

7.1 The review established that there are **twenty three** extant section 94 directions within the scope of IOCCO's oversight[17].

7.2 These twenty three directions were all given by the Home Secretary or Foreign Secretary at various times between 2001 and 2016 on behalf of the Security Service, GCHQ, the three agencies collectively (Security Service, GCHQ and SIS) or on behalf of the MPS CTC.

7.3 All of the section 94 directions specified that they were necessary under section 94(1) of the Telecommunications Act 1984 *"in the interests of national security"*. None of the section 94 directions specified that they were necessary for *"relations with the government of a country or territory outside the United Kingdom"*.

7.4 **Fifteen** of the twenty three extant section 94 directions relate to the acquisition of bulk communications data. Only GCHQ and the Security Service have section 94 directions to acquire bulk communications data. See **section 8** of this report for our review of those directions.

7.5 The remaining **eight** extant section 94 directions were given on behalf of the Security Service, the three agencies collectively, or the MPS CTC. These relate to the provision of services in emergencies, for civil contingency purposes or to help the agencies in safeguarding the security of their personnel and operations. See **section 9** of this report for our review of those directions.

[17] See paragraphs 2.5 and 2.7 of this report for the scope of IOCCO's oversight of section 94 directions.

Section 8

Review of section 94 directions to acquire bulk communications data

8.1 This section of the report details the findings in relation to our review of section 94 directions to acquire bulk communications data.

Definitions

8.2 **Communications data**

8.3 Communications data colloquially embraces the 'who', 'when' and 'where' of a communication but not the content, not what was said or written. Put shortly, communications data comprise the following:

- ***Traffic data*** are data that may be attached to a communication for the purpose of transmitting it and could appear to identify the sender and recipient of the communication, the location from which and the time at which it was sent, and other related material (see sections 21(4)(a) and 21(6) and (7) of RIPA and Paragraphs 2.24 to 2.27 of the code of practice for the Acquisition and Disclosure of Communications Data[18]).
- ***Service use information*** is data relating to the use made by any person of a communication service and may be the kind of information that habitually used to appear on a itemised billing document supplied to customers (see section 21(4)(b) of RIPA and Paragraphs 2.28 and 2.29 of the code of practice for the Acquisition and Disclosure of Communications Data)[19].

---

[18] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/426248/Acquisition_and_Disclosure_of_Communications_Data_Code_of_Practice_March_2015.pdf

[19] See footnote 18

- ***Subscriber information*** is data held or obtained by the provider of a communications service in relation to a customer and may be the kind of information which a customer typically provides when they sign up to use a service, for example, the recorded name and address of the subscriber of a telephone number or the account holder of an email address. (See section 21(4)(c) of RIPA and Paragraphs 2.30 and 2.38 of the code of practice for the Acquisition and Disclosure of Communications Data)[20].

8.4 **Personal data**

8.5 There have been several public consultations undertaken in relation to the retention and use of communications data by public authorities.

8.6 In March 2003 the Government published a *"Consultation on a Code of Practice for the Voluntary Retention of Communications Data"*[21] (accompanying the Anti-Terrorism, Crime & Security Act 2001) and acknowledged that communications data (within the meaning of section 21(4) of RIPA 2000) was personal data within the meaning of the Data Protection Act 1998:

- *"...the retention of data is processing therefore to comply with the principles of the Data Protection Act 1998 the data must not be kept for longer than is necessary..."*
- *"...the lengthy discussions between the Home Office and the Information Commissioner's Office have produced agreement that the processing, and as indicated in the previous paragraph retention itself is a form of processing, of data retained under the Anti-terrorism, Crime & Security Act 2001 will fall within paragraph 5 of schedule 2 of the DPA. Similarly, where any data retained under the Code constitutes sensitive personal data its processing is permitted by virtue of paragraph 7(b) of schedule 3 DPA."*

consequence of the ongoing case[28] before the IPT referred to earlier in section 3 of this report.

Why has communications data been acquired in bulk by the agencies using a section 94 direction rather than under Chapter 2 of Part 1 of RIPA?

8.18 A series of 12-year old correspondence[29] between Home Office and GCHQ lawyers and a former Commissioner (from 2004) has been disclosed as part of the aforementioned IPT case.

8.19 The correspondence shows that in June 2004 the Home Office carried out a legal analysis of Chapter 2 of Part 1 of RIPA and section 94 of the Telecommunications Act 1984 and concluded that the purpose of Chapter 2 of Part 1 RIPA is to make lawful the acquisition and disclosure of communications data which would otherwise be unlawful. However, if a direction is made under section of the 94 of the Telecommunications Act 1984, the acquisition of the data from the PECN would also be lawful (to the extent required by Article 1 of Protocol No 1 ECHR) and there would therefore be no need to use Chapter 2 of Part 1 RIPA.

8.20 On this basis, the transfer from the PECN to the agencies could be made lawful under Chapter 2 of Part 1 RIPA or under section 94 of the Telecommunications Act 1984. The Home Office correspondence sets out that the practical or even presentational difference between the two provisions is that if Chapter 2 of Part 1 RIPA were used, a new notice would need to be given every month (in accordance with the renewal provisions of section 23 of RIPA) whereas a section 94 direction is given once and is of indefinite duration.

8.21 The Home Office's analysis that the use of section 94 directions is a more appropriate instrument to Chapter 2 of Part 1 of RIPA was based on two factors:

- Section 94 directions would be given by the Home Secretary and would be subject to legal advice from the Home Office, whereas a notice given under Chapter 2 of Part 1 RIPA would be considered by an official within the public authority (in accordance with the then Regulation of Investigatory Powers (Communications Data) Order 2003 (SI 2003/3172)). Even if the notice were given by the head of an intelligence agency, it

[28] Privacy International v. Secretary of State for Foreign & Commonwealth Affairs et al. – IPT/15/110/CH
[29] https://privacyinternational.org/sites/default/files/IOCCO%20Correspondence%202004.pdf

would always be issued by a member of the public authority rather than the Home Secretary who, as in the case of interception warrants, is accountable to Parliament. A decision of this significance ought to be taken by a politician who is directly accountable to Parliament, rather than a senior member of a public authority; and

- Although there is nothing to prevent Chapter 2 of Part 1 RIPA being used in this way it would, over time, be likely to act as a precedent so that other public authorities could attempt to meet the necessity and proportionality test to acquire bulk communications data.

8.22 The Home Office also indicated that, as permitted by section 94(4), because of the national security issues it was not intended that the section 94 direction(s) would be laid before Parliament.

8.23 The then Commissioner (in 2004) was eventually persuaded by these arguments and agreed that the acquisition of the communications data by either section 94 of the Telecommunications Act 1984 or by Chapter 2 of Part 1 of RIPA was lawful, and that the appropriate way to access communications data already obtained pursuant to a section 94 direction would be for the Security Service to use an authorisation[30] under Chapter 2 of Part 1 of RIPA.

8.24 There was then correspondence between GCHQ lawyers and the then Commissioner in October and November of 2004 setting out the different procedure in place within GCHQ to access data acquired pursuant to section 94 directions. This procedure is set out in more detail later in this report, but the then Commissioner stated that he was content that the system within GCHQ for the retrieval of data pursuant to section 94 directions was lawful.

8.25 In relation to the giving of a section 94 direction, the historic correspondence did not address the wording or genesis of section 94 of the Telecommunications Act 1984 or take full account of the ECHR, in particular the principle of legal certainty, or legality. The Home Office advice does not acknowledge that the transfer and storage of the communications data from the PECN to the agency may constitute an interference with Article 8 of the ECHR and asserts that the first infringement of Article 8 would be at the stage the agency accesses the data already retained. As a result, the Home Office advice did not provide an analysis as to why the

[30] Essentially there are two methods for acquiring communications data under RIPA – an authorisation under section 22(3) or a notice under section 22(4). An authorisation is effected by a person from the relevant public authority engaging in conduct to acquire the communications data. A notice is effected by requiring a CSP to disclose the data to the relevant public authority.

interference at the acquisition stage (using section 94 directions) was deemed to be in accordance with Article 8 of ECHR. The historic correspondence does not recognise that bulk communications data is personal data or refer to the Council of Europe's 2002 *"Guidelines on human rights and the fight against terrorism"*, in particular section 5 of those Guidelines which relate to the collection and processing of personal data by any competent authority in the field of state security (see paragraph 8.11 of this report).

8.26 As set out in paragraph 3.3 of this report, our review of section 94 directions did not seek to determine whether the section 94 regime is sufficiently clear and accessible as this is the exclusive role of the IPT. We do not therefore intend to stray into the legal arguments around this point as it is already being considered, and will be determined, by the IPT in the case currently before it. Suffice to say that our review of this historic correspondence, taking into account the case law and guidance that was available at the time[31], shows its consideration of the legal issues to have been incomplete. We do not know whether there was consideration given to the legal issues otherwise than as disclosed by the correspondence we have seen.

The operational case for bulk communications data being acquired and retained by the agencies

8.27 The Government has sought recently to explain the operational requirement for bulk communications data in a paper entitled "Operational Case for Bulk Powers"[32]:

> *"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.*

[31] See for example in particular Malone v UK (App 8691/79 (1985) 7 EHRR 14, the Rechnungshof cases (Joined Cases C-465/00, C-138/01 and C-139/01) and the Council of Europe Guidelines referred to at paragraph 8.11 of this report.
[32] See section 9 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/504187/Operational_Case_for_Bulk_Powers.pdf

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.

In some cases bulk communications data may be the only investigative lead that the security and intelligence agencies have to work with. 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. 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."

8.28 We note that David Anderson QC, the Independent Reviewer of Counter Terrorism legislation, has recently been asked by the Home Secretary to carry out a review of the operational case for all of the bulk powers in the Investigatory Powers Bill[33]. That review will include the operational case for the power to acquire bulk communications data.

8.29 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 made under Chapter 2 of Part 1 of RIPA.

8.30 It would be helpful if the legislation and policy clarified whether it is necessary (or appropriate) for the agencies to access the bulk communications data obtained pursuant to section 94 directions where there is no need to carry out complex analysis, for example, where

[33] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/527764/TOR_for_Bulk_Review.pdf

a targeted request is made against a communications address linked to a subject of interest i.e. "location and call data for a period of one month on a known communications address".

8.31 The agencies submit that the speed at which individual data requests (once authorised under Chapter 2 of Part 1 of RIPA) can be acquired from the communication service providers (CSPs), using the secure online workflow systems[34] developed for this purpose, is not sufficient for them to meet their operational requirements. This will no doubt be the case where there is an urgent need to acquire communications data in relation to an immediate and credible threat to national security, but it is arguably not the case when dealing with more routine requests which, within the agencies, form the majority. The secure online workflow systems have developed significantly in the past few years, both in terms of the speed of disclosure and the types of communications data available on the systems. These developments are likely to continue and therefore this should be kept under review.

8.32 Later in this section of the report we set out the procedures that the agencies have put in place to access the bulk communications data acquired pursuant to section 94 directions.

The nature of the section 94 directions for bulk communications data

8.33 Fifteen section 94 directions for bulk communications data given between 2001 and 2012 are extant. Although these fifteen remain in force, the review identified that a number of the directions have been modified over the years, for example, to expand or to cease the acquisition of certain data, and this has led in some instances to the direction being re-issued (see paragraphs 8.42 and 8.52 below). Furthermore, the submissions relating to one of the 2001 directions made reference to the fact that it was superseding a previous direction originally issued in 1998.

8.34 All of the extant requirements for bulk communications data are for traffic data as defined in section 21(4)(a) of RIPA[35]. All of the current directions require regular feeds of bulk communications data to be disclosed by the relevant PECN.

[34] See Para 7.104 of our March 2015 report for an explanation of these systems http://www.iocco-uk.info/docs/IOCCO%20Report%20March%202015%20(Web).pdf
[35] See section 8.3 of this report

8.35 IOCCO identified that a PECN had historically been required (since 2001) to supply *subscriber information*[36] to GCHQ in addition to *traffic data* as part of a section 94 direction. The *subscriber information* requirement ceased in August 2015 after an internal review. GCHQ has confirmed that the subscriber information obtained pursuant to this section 94 direction was destroyed in October 2015. The *Operational Case for Bulk Powers* published in March 2016 by the Government[37] does not set out an operational requirement or case for bulk subscriber information. The agency handling arrangements[38] for the acquisition of bulk communications data published in November 2015 state clearly that:

> *"The communications data collected is limited to "Traffic Data" and "Service Use Information".*
>
> *"The data provided does not contain communication content or Subscriber Information..."*

8.36 Both of the documents referred to in the preceding paragraph were published after the requirement for subscriber information had ceased. In this review we did not identify any extant requirements for PECNs to disclose bulk subscriber information.

Findings relating to the examination of the section 94 directions and accompanying submissions to the Secretary of State to acquire bulk communications data

8.37 In the absence of any codified procedures in or made pursuant to section 94 of the Telecommunications Act 1984, the agencies have developed a process to facilitate the acquisition of bulk communications data and to review and provide operational updates in relation to the use of section 94 directions for bulk communications data. That process is set out in the handling arrangements[39] published by the agencies in November 2015 and includes a number of the elements described in paragraphs 4.14 and 4.15 of this report.

---

[36] see section 8.3 of this report

[37] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/504187/Operational_Case_for_Bulk_Powers.pdf

[38] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473780/Handling_arrangements_for_Bulk_Communications_Data.pdf

[39] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473780/Handling_arrangements_for_Bulk_Communications_Data.pdf

8.38 The process can be broken down into four distinct areas, some of which may be undertaken simultaneously:

a) The agency identifies and describes the bulk communications data considered necessary to meet its operational objectives;
b) The agency identifies the relevant PECN(s) and consults to assess whether the acquisition of specific communications data in bulk from a PECN is reasonably practical or whether the specific data required is inextricably linked to other data;
c) The agency consults further with the PECN and assesses whether the data can be made available by means of a section 94 direction; and
d) The agency determines whether the bulk acquisition of communications data is appropriate under a section 94 direction and, if so, prepares a detailed submission for consideration by the Secretary of State.

8.39 The submissions supporting the acquisition of bulk communications data under a section 94 direction are highly detailed. They explain why the acquisition of the bulk communications data is required in the interests of national security, giving information about the operational requirement or intelligence gap that the agency is seeking to address. They provide an explanation of the relevant data to be acquired and the proposed action. The submissions, when addressing the issue of proportionality, give extensive detail as to how the data will assist to address the operational requirement, the expected value of the intelligence to be derived from the data and why there is no other appropriate or suitable alternative to the proposed direction.

8.40 The submissions make explicit that once acquired the data will only be accessed and handled in accordance with the Security Service Act (1989), the Intelligence Services Act (1994), the Counter-Terrorism Act (2008) and the handling arrangements[40]. The submissions also outline the case for the Secretary of State to exercise their discretion and not lay the particular direction in Parliament, which in general terms is because disclosure was thought to be against the interests of national security and the commercial interests of the relevant PECN. The submissions also contain a risk assessment as to the consequences of such a disclosure.

---

40 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473780/Handling_arrangements_for_Bulk_Communications_Data.pdf

8.41 Each Secretary of State has Senior Officials and staff in their respective Government departments whose functions include scrutinising applications for bulk communications data directions for their form, content and sufficiency, and presenting them to the relevant Secretary of State with appropriate advice.

8.42 The form and content of the actual section 94 directions issued for bulk communications data by the Security Service and GCHQ differed in the following ways:

- Security Service section 94 directions (given by the Home Secretary) were:
  - highly detailed and contained specific information about the data sought, either by description or the technical naming of the data; and
  - stated that any amendment to an existing data requirement required a new section 94 direction to be given by the Secretary of State to supersede the existing section 94 direction.

- GCHQ section 94 directions (given by the Foreign Secretary):
  - were very broad and provided a general description of communications data which was far wider than the requirement actually made of the PECN; and
  - the supporting documentation accompanying the section 94 direction then gave the specific details of the *actual data sought* including either by description and / or by the technical naming of the data; and
  - the supporting documentation containing the specific data requirements has from time to time been modified to amend a data requirement (i.e. to extend or to cease certain data). Each modification has been submitted to the Foreign Secretary for authorisation, but the section 94 directions themselves have not been amended or re-issued.

8.43 There is no doubt that the lack of a codified process in or under the Telecommunications Act 1984 relating to the application process and to the form and content of a section 94 direction for bulk communications data has led to these two different processes.

8.44 Section 94 of the Telecommunications Act 1984 enables the Secretary of State to give a direction of a "general character". In our view any legal requirement given to a PECN for bulk communications data should indicate the *specific* communications data that is required

to be disclosed. It is unsatisfactory to have a direction which provides a general description that is broader than the communications data that the PECN is actually being required to disclose. Furthermore the fact that a new section 94 direction has not been given each time a data requirement has been modified made the process more disjointed and difficult to audit.

8.45 Recommendation 3: All section 94 directions for bulk communications data should indicate the specific communications data that is required to be disclosed by the PECN. When a requirement is amended (i.e. modified) a new direction should be given.

8.46 Recommendation 4: There should be a clear mandated application process for section 94 directions which sets out the requirements to be met. The public authorities (in consultation with the Home Office and Foreign & Commonwealth Office) should develop a specimen application form template and a specimen section 94 direction template in order to ensure a standard and consistent approach.

The giving of a section 94 direction for bulk communications data to a PECN

8.47 When the Secretary of State has given a section 94 direction the PECN is informed of the decision and a copy of the direction is either served or made available for inspection by the PECN (the latter if they are unable to store the direction securely). Only the section 94 direction is served on the PECN. The supporting submission presented to the Secretary of State is retained by the Home Office and Foreign & Commonwealth Office and the relevant agency.

8.48 Notwithstanding the differences between the form and content of the section 94 directions referred to previously, all of the PECNs were satisfied overall that the section 94 directions and supporting documentation sufficiently explained what conduct they were required to undertake, what data they were being required to disclose and the mechanisms involved.

8.49 IOCCO identified that where a PECN had changed its company name and / or had merged with another PECN the Security Service had not amended its section 94 direction to reflect the change. GCHQ had however made such amendments over the years. In our view any legal requirement given to a PECN, or maintained in relation to it, should correctly name the PECN.

8.50 Recommendation 5: Where a PECN changes its company name or merges with another PECN, a new section 94 direction must be given to reflect the change.

Review, modification and cancellation provisions for section 94 directions for bulk communications data

8.51 As mentioned earlier, there are no duration or review requirements in section 94 of the Telecommunications Act 1984. However we established from the documents examined in this review that the Security Service and GCHQ submit updates to the Secretary of State confirming that internal six-monthly reviews have been undertaken to assess whether the reasons and justifications for the section 94 directions remain valid. In addition, the Security Service, as part of its ongoing liaison with the PECNs, provides details of the operational benefit derived and the use made of the data. The PECNs are also informed by the Security Service and by GCHQ of their obligation to continue to comply with the section 94 directions.

8.52 Furthermore, although there is no formal statutory mechanism for the cancellation of a section 94 direction, the agencies in practice have informed both the Secretary of State and the PECN when they no longer require the bulk communications data to be disclosed. In some instances a particular data requirement has been modified or ceased. Again there is no statutory mechanism for a section 94 direction to be modified but in all cases a submission was sent to the Secretary of State setting out the justification for the change and the agency consulted with the PECN in the same way as it would with a new section 94 direction.

8.53 Recommendation 6: There should be a clear written mandated process for the review, modification and cancellation of any section 94 directions. The public authorities (in consultation with the Home Office and Foreign & Commonwealth Office) should develop specimen templates for the submission of reviews, modifications or cancellations to the Secretary of State to ensure a standard and consistent approach. In the absence of any statutory provision to modify a section 94 direction, a new direction should be issued as per Recommendation 3.

Findings relating to the acquisition and retention of the bulk communications data

8.54 On several occasions we met and spoke at length with those involved in the secure electronic transfer of communications data from the PECNs to the agencies and those who administer and control the retention, access to and finally the destruction of the data. The individuals with whom we engaged included senior managers, experts involved in the architectural design of the systems and analysts who sought access to the data to carry out their intelligence functions.

8.55 We determined that the agencies had applied the protective security measures set out in the handling arrangements[41]. Specifically, in relation to the secure electronic transfer of the bulk communications data to the agencies and its storage we established:

- data is stored on servers within highly secure locations and is subject to significant layers of physical security with onsite and remote security monitoring;
- all members of staff involved in the processes are security vetted at Developed Vetting (DV) level i.e. for staff dealing with matters considered to be Secret and Top Secret;
- all members of staff involved in the processes are named individuals, i.e., knowledge / involvement is not determined simply by the post held, and access ceases when they move post;
- a 6-monthly review is undertaken to assess design architecture and physical security;
- a small number of named staff are involved in managing raw data as it is imported into the architecture;
- in terms of retention and destruction; the Security Service holds the communications data acquired pursuant to a section 94 direction for a period of 365 days, automatically deleting it on a daily basis. GCHQ's policy is to hold communications data acquired pursuant to section 94 directions for a maximum of 1 year. In practice the retention limit is lower than this, and the data is subject to automated deletion on a daily basis.

[41] See section 4.3 in particular- https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473780/Handling_arrangements_for_Bulk_Communications_Data.pdf

8.56 There was also documentary evidence that the agencies had considered and implemented procedures which took account of other legislation affecting the manner in which the data was acquired and retained (for example, the Data Protection Act 1998).

8.57 The agencies are each a *"data controller"* and are required by section 4(4) of the DPA to comply with the data protection principles in Part 1 of Schedule 1 (subject to exemption by ministerial certificate) and are in any event not exempted from the obligation to comply with the 5th and 7th data protection principles, which provide:

> *"(5) Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes..."*
> *"(7) Appropriate technical and organisation measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data..."*

Access to the bulk communications data retained by the agency

8.58 In order to examine the procedures in place to access the data for operational purposes we engaged with those in charge of intelligence operations, those senior managers authorising access, analysts within operational teams and those who manage and undertake audits of the access.

8.59 We established that two distinct processes have developed within the Security Service and GCHQ to access bulk communications data, both of which include consideration of the principles of necessity and proportionality as set out below. Because of the different procedures in place within those two agencies to access the bulk communications data acquired pursuant to section 94 directions it is not possible to provide comparable statistical information relating to the access and use of the bulk communications data. In the following paragraphs of this report we set out the two distinct processes and provide some statistical information about the use made of these directions by both agencies.

8.60 GCHQ

8.61 Within GCHQ, all operational data gathered from a variety of different sources is treated in the same manner. Where there is an operational requirement to gain access to operational data (which will include bulk communications data), an *analyst* is required to

justify why the access and examination of the data are necessary and proportionate. This is a three-stage process covering:

- why the search is necessary for one of the authorised purposes, for example, *"in the interests of national security"*;
- an internal cross-reference number which equates to the intelligence requirement and priority for the search;
- a justification of the necessity and proportionality to access the data.

8.62 We carried out investigations into the selection of bulk communications data for examination by analysts at GCHQ by reviewing the breadth and depth of the internal procedures and by auditing a number of individual requests made by analysts. We were satisfied that in the individual requests examined the analysts had justified properly why it was necessary and proportionate to access the communications data. In 2015 GCHQ identified 141,251 communications addresses or identifiers of interest from communications data acquired in bulk pursuant to section 94 directions which directly contributed to an intelligence report.

8.63 In previous IOCCO reports[42] we have commented on the process within GCHQ for the selection and examination of intercepted material and related communications data[43]. The process for the selection and examination of bulk communications data is essentially the same. We therefore draw the same conclusion that, although the selection procedure is carefully and conscientiously undertaken both in general and, so far as we were able to judge, by the individuals concerned, the process relies mainly on the professional judgment of analysts, their training and management oversight. There is no pre-authorisation or authentication process to allow access to bulk communications data that has already been acquired and retained by the agency under a section 94 direction.

8.64 GCHQ has however implemented retrospective audit checks. The senior managers we interviewed as part of this review explained in detail how the audit processes work and the function of GCHQ's Internal Compliance Team who carry out *ex-post facto* random audit checks of the analysts' justifications for the selection of bulk communications data. In

[42] See for example Paragraphs 6.37 to 6.40 of the March 2015 Report http://www.iocco-uk.info/docs/IOCCO%20Report%20March%202015%20(Web).pdf

[43] See section 20 of the Regulation of Investigatory Powers Act 2000 for definitions of "intercepted material" and "related communications data" http://www.legislation.gov.uk/ukpga/2000/23/section/20

addition, GCHQ's IT Security Team conducts technical audits to identify and further investigate any possible unauthorised use[44].

8.65 The Security Service

8.66 The Security Service has developed a policy and procedure for accessing the bulk communications data (acquired and retained by the agency as a consequence of section 94 directions) which substantially mirrors that set out in Chapter 2 of Part 1 of RIPA and the code of practice for the Acquisition and Disclosure of Communications Data.[45]

8.67 The investigator / analyst sets out in an application why it is necessary and proportionate to gain access to the data. The giving of authority for access to the data retained by the Security Service is undertaken by a designated person[46] (DP) of appropriate seniority within the Security Service. The designated persons undertaking this function are generally *not independent* from the investigations to which the requests they are authorising relate and they generally *do not* record any written considerations when approving such requests. Anyone familiar with the code of practice for the Acquisition and Disclosure of Communications Data would recognise these two features as requirements when communications data is acquired using RIPA from communication service providers (CSPs). There are exceptions to this within the Security Service's policy, for example, when communications data relating to the communications of an individual known to be a member of a profession that handles privileged or otherwise confidential information is accessed, the Security Service's policy stipulates that the designated person considering the request must be independent.

8.68 As part of this review we examined a number of the applications submitted by investigators or analysts to gain access to bulk communications data. It is important to point out that in the main there is no procedural difference when a Security Service investigator / analyst applies to access bulk communications data already obtained pursuant to a section 94 direction or applies to acquire communications data under Chapter 2 of Part 1 of RIPA from a CSP.

---

[44] See page 26 (paragraph 6.39) http://iocco-uk.info/docs/IOCCO%20Report%20March%202015%20(Web).pdf

[45] See Chapter 3 – The General Rules on the Granting of Authorisations and Notices https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/426248/Acquisition_and_Disclosure_of_Communications_Data_Code_of_Practice_March_2015.pdf

[46] A **designated person**, is a person holding a prescribed office in the relevant public authority, who must decide whether it is lawful, necessary and proportionate to acquire the communications data to which the application relates. Their function and duties are described in paragraphs 3.7 to 3.14 of the code of practice for the acquisition and disclosure of communications data. Except where it is unavoidable or for reasons of urgency or security, the designated person should not be directly involved in the relevant investigation.

8.69 We had access to the system predominantly used by investigators and analysts within the Security Service to apply to access the bulk communications data and were able to undertake *random sampling* and run *query-based searches*[47] on that system to, for example, evaluate the analysts' / investigators' necessity and proportionality considerations, examine particular operations, identify requests for more intrusive data sets or those requiring data over extended time periods etc.

8.70 In 2015 the Security Service made 20,042 applications to access communications data obtained pursuant to section 94 directions. These applications related to 122,579 items of communications data[48]. Overall we concluded that the Security Service applications that we examined were submitted to an excellent standard and satisfied the principles of necessity and proportionality.

Acquisition and access errors

8.71 There is no statutory requirement under section 94 of the Telecommunications Act 1984 to report an error when-

a) undertaking the acquisition of bulk communications data by means of a section 94 direction, or

b) when accessing data already retained as a consequence.

8.72 The Security Service

8.73 The Security Service has however developed and implemented an internal policy process to report to IOCCO instances they consider to be errors under (b) above which cause communications data to be accessed wrongly.

8.74 Between 1st January 2015 and the date of the completion of this report the Security Service reported 230 errors to us.

[47] Query based searches involve inquiries against defined criteria or subjects. See paragraphs 7.36 to 7.39 of our March 2015 Report for more on random and query based searches http://www.iocco-uk.info/docs/IOCCO%20Report%20March%202015%20(Web).pdf

[48] See Paragraph 6.5(K) of the acquisition and disclosure of communications data code of practice which defines one item of communications data as a single communications address or other descriptor included within an application.

8.75 A breakdown of the causes of the errors reported to IOCCO is as follows;

- 14 errors were caused by the applicant (i.e. the investigator / analyst) acquiring data on an incorrect communications address or identifier;
- 5 errors were caused by the applicant acquiring communications data over an incorrect date / time period;
- 1 error was caused by excess data being acquired which fell outside the scope of the authorisation;
- a series of 210 errors were caused by a failure to comply with the Security Service's handling arrangements.

8.76 The 210 instances (described above) took place between 2010 and early May 2016, when the Security Service discovered that their handling arrangements and internal policies had not been followed in a number of instances when access to the bulk communications data had been authorised. A DP within the Security Service first identified several instances of the policies not being followed and reported the contraventions of the Security Service's handling arrangements and processes for accessing communications data acquired in bulk to the compliance investigations team. The Security Service initiated an immediate review of the process and identified the wider instances which, in their policy terms, constitute errors because communications data has been accessed without following the internal procedures. This review is ongoing at the time of the completion of this report.

8.77 In these instances the *written record* of the necessity and proportionality case to access the bulk communications data was made after the authorisation had been given orally by a DP or was incomplete. The written application should have been completed prior to access being undertaken, as is normally the case (and which is something we confirmed in our investigation).

8.78 IOCCO has conducted an investigation into this series of 210 errors. As part of our investigation we examined all of the documentation relating to these instances and interviewed managers, analysts, investigators, lawyers, DPs and individuals involved in internal audits of the relevant systems.

8.79 Overall we are satisfied from our investigation that the communications data accessed in these instances was accessed for legitimate purposes, i.e. in relation to the Security Service

pursuing their functions as set down in the Security Services Act 1989[49]. We are also satisfied, as far as we can be from the interviews and the records we examined, that the case to access the communications data was made orally and was authorised by a DP prior to the data being accessed (for example, we examined operational notes on file and other records indicating an oral briefing to the DP had taken place). We found no evidence that the applications which were completed retrospectively did not meet the tests of necessity or proportionality. In a very small number of these cases it appears that there was an urgent operational requirement to access the communications data and there was no time to complete the normal written process, but this is not the case for the vast majority.

8.80 These conclusions aside, these instances represent clear contraventions of the handling arrangements[50] and the Security Service's internal policies concerning access to bulk communications data retained pursuant to a section 94 direction. Paragraph 1.3 of the handling arrangements specifies that *"failure by staff to comply with these Arrangements may lead to disciplinary action, which can include dismissal and prosecution"*. We have evaluated the measures that have already been implemented by the Security Service to prevent recurrence and a number that are still under consideration. We have also made a number of recommendations to the Security Service to prevent recurrence, for example, recommendations concerning the training and guidance issued to analysts and managers and enhancements to the audit processes. As mentioned above, the Security Service's review of these matters is still ongoing.

8.81 In all instances where communications data retained in bulk is accessed wrongly by the Security Service and is not of national security interest, the copy of the data extracted for analysis is destroyed.

8.82 GCHQ

8.83 As previously stated, GCHQ in the main merges the communications data obtained under a section 94 direction with other datasets containing communications data (for example, related communications data[51] obtained as a consequence of an interception warrant). GCHQ have a mechanism for reporting errors to the Commissioner, but cannot

[49] See sections 1 and 2 http://www.legislation.gov.uk/ukpga/1989/5/contents

[50] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473780/Handling_arrangements_for_Bulk_Communications_Data.pdf

[51] See section 20 of the Regulation of Investigatory Powers Act 2000 for definition of "related communications data" http://www.legislation.gov.uk/ukpga/2000/23/section/20

9.4 These directions do not require the PECNs to disclose bulk communications data. All of these "other" directions require PECNs to undertake conduct to do or not to do a particular thing specified in the direction.

9.5 A number of the "other" directions are in place to ensure that there is provision in emergencies or for civil contingency purposes. In these cases, for example, PECNs might be directed to maintain a continuous capability to enable them to be able to undertake certain specific conduct as and when they are required to do so. These directions, by their very nature, are put to use infrequently.

9.6 Some of the "other" directions require the PECNs to take preparatory steps in order to, for example, provide a continuous capability to be used in emergencies. By preparatory steps we mean that the directions are not normally used for the primary purpose of interfering with privacy and do not normally result in the acquisition of personal data. In instances where there is potential for interference with privacy to occur, the public authority seeks another authorisation to approve this interference. It is worth noting that at present that second authorisation may fall outside of IOCCO's oversight remit. For example, it could be an authorisation to interfere with property and, in such a case the subsequent authorisation would be under the remit of the Intelligence Services Commissioner or the Office of the Surveillance Commissioners' (OSC) depending [redacted]

examination of these eight "other" section 94 directions and the supplementary documentation we can state that the processes followed are similar to those for section 94 directions to acquire bulk communications data.

9.9 The submissions supporting the section 94 directions were highly detailed. They set out why the PECN is being, or may be, required to undertake conduct in the interests of national security and why that conduct is necessary and proportionate. The submissions outline the case for the Secretary of State to exercise their discretion and not lay the direction in Parliament, which in general terms is because disclosure was thought to be against the interests of national security or the commercial interests of the relevant PECN. The submissions have been reviewed every six months by the relevant public authorities. Recommendations 1 to 4 of this report (see paragraphs 5.13, 5.14, 8.45 and 8.46) are equally relevant to these directions.

The giving of "other" section 94 directions

9.10 The section 94 directions themselves are very detailed and specified clearly the conduct that the PECN was being, or might be, required to undertake under the direction. We confirmed that all of the PECNs were satisfied overall that the section 94 directions and supporting documentation explained what conduct they were or may be required to undertake and the mechanisms involved.

9.11 When the Secretary of State has given a section 94 direction the PECN is informed of the decision and a copy of the direction is either served or made available for inspection by the PECN (the latter if they are unable to store the direction securely). Only the section 94 direction is served on the PECN. The supporting submission presented to the Secretary of State is retained by the Home Office and Foreign & Commonwealth Office and the relevant agency. Recommendation 5 of this report (see paragraph 8.50) is equally relevant to these directions.

Review, modification, cancellation and error reporting provisions for "other" section 94 directions

9.12 As mentioned earlier, there are no duration or review requirements in section 94 of the Telecommunications Act 1984. However we established from the documents examined as

part of this review that the "other" directions have been reviewed every six months. The PECNs are also informed by the agency or other public authority of their obligation to continue to comply with these section 94 directions.

9.13 Furthermore, although there is no formal statutory mechanism for the cancellation of a section 94 direction, the agencies in practice have informed both the Secretary of State and the PECN should they no longer require the conduct to be undertaken. In some instances a particular requirement has been modified or ceased. There is no statutory mechanism for a section 94 direction to be modified or revised but in all cases a submission was sent to the Secretary of State setting out the justification for the change and the public authority consulted with the PECN in the same way as they would for a new section 94 direction. There are also no procedures for the reporting of errors that may occur in the giving of or compliance with a section 94 direction. Recommendations 6 and 7 of this report (see paragraphs 8.53 and 8.84) are therefore equally relevant to these "other" directions.

What will the IOCCO oversight regime for "other" section 94 directions look like?

9.14 On an annual basis we intend to carry out formal inspections within any public authorities for which the Secretary of State has given "other" section 94 directions. At present those are only the three intelligence agencies collectively, the Security Service alone or the MPS CTC. Those inspections and audits will cover the following phases:

- the giving of section 94 directions by the Secretary of State requiring PECNs to undertake conduct (including a review of the judgements made by the secretary of state and the public authority relating to necessity and proportionality);
- the serving of any "other" section 94 directions on the PECNs, including the prior consultations between the public authorities and PECNs and any subsequent communication;
- liaison, where relevant, with other oversight bodies (such as the Intelligence Services Commissioner or OSC) to check properly that a separate authorisation has been given to interfere with privacy;
- a review of the errors reported and measures put in place to prevent recurrence.

- consultation with the PECN (or "operator" in IP Bill terms) to ascertain whether the steps required to give effect to a bulk acquisition warrant or national security notice are limited to those which it is reasonably practicable to take;
- the giving of a technical capability notice for an operator to provide a technical capability to facilitate compliance with a bulk acquisition warrant. There is an obligation to consult with the operator beforehand and a referral procedure if the operator considers the requirements placed on them in such a notice are unreasonable;
- the security, dissemination, copying, storage and transfer and destruction of the data;
- the selection and examination of bulk communications data (including special procedures for individuals who hold sensitive professions or where the data is selected for examination in order to determine the source of journalistic information);
- record keeping arrangements, including retention of all applications and associated documentation and statistical information about bulk acquisition warrants;
- reporting of errors which occur during the acquisition, disclosure or access to (i.e. selection for examination) bulk communications data; and,
- oversight by the Investigatory Powers Commissioner which includes an obligation to provide the Commissioner with all necessary assistance, including unfettered access to all locations, documentation and information systems as required to carry out their full function.

10.4 All of the PECNs welcomed the opportunity to codify the procedures and requirements for conduct currently undertaken under section 94 directions in the IP Bill and, as currently drafted, the draft codes of practice will go a significant way to do that.

Section 11

Summary and conclusions

11.6 This review has been challenging for a number of reasons. First, the section 94 directions are secret as allowed for by statute. During our drafting of this report we have had to be mindful of the fact that none of the section 94 directions under our oversight have been laid in Parliament by the Secretary of State and therefore they remain subject to the statutory secrecy provisions. These restrictions also apply to the public authorities and PECNs. This severely limits what we can say about the nature of the directions and the conduct undertaken in pursuance of any direction.

11.7 Secondly, section 94 of the Telecommunications Act 1984 does not include any provision for independent oversight or any requirements for the keeping of records. We did receive full cooperation from staff within the public authorities and the PECNs when carrying out this review. However it was challenging for us to piece together and determine historically what section 94 notices had been given, by whom and when, and whether they were still in force. We are however satisfied that we now have a comprehensive record of the twenty three extant section 94 directions and the conduct undertaken by the PECNs in relation to those directions.

11.8 Thirdly, section 94 of the Telecommunications Act 1984 does not include any provision for the Secretary of State to issue codes of practice for the exercise or performance and duties relating to section 94 directions. Such codes of practice would include provision for the application, authorisation, review, modification and cancellation of any directions. For bulk communications data a code of practice would likely include provision for the subsequent use, retention and destruction of bulk communications data acquired pursuant to any such directions. The provisions in the Investigatory Powers Bill, the Bulk Acquisition: Draft Code of Practice and the National Security Notices: Draft Code of Practice as drafted are an opportunity to remedy this.

11.9 In order to remedy the lack of provisions in or under section 94 of the Telecommunications Act 1984 the public authorities have developed procedures to facilitate applying to a Secretary of State for section 94 directions and to review, modify and cancel section 94 directions. However until the publication of the handling arrangements[58], the procedures relating to bulk communications data section 94 directions were operated in secret and were overseen on a *limited* and non-statutory basis by two different Commissioners. Where the section 94 directions do not relate to the acquisition of bulk

58 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473780/Handling_arrangements_for_Bulk_Communications_Data.pdf

communications data there are no published arrangements concerning the processes to be followed. In these cases we confirmed that the procedures being followed are similar to those in place for bulk communications data, but there was no oversight of these "other" directions in place before the Prime Minister directed that the Commissioner should extend his oversight to these directions in 2015.

11.10 It is unsurprising that the lack of a codified process in or under section 94 of the Telecommunications Act 1984, along with the different functions and missions of GCHQ and the Security Service, have led to a number of dissimilar processes evolving within those agencies relating to section 94 directions to acquire bulk communications data, for example, the procedures relating to the form and content of section 94 directions and the procedures to access the bulk communications data acquired pursuant to any section 94 directions. We were satisfied that the agencies had introduced comprehensive procedures in accordance with the handling arrangements to ensure that they only acquired and retained bulk communications data and then accessed and undertook analysis of that data in order to pursue their functions as set out in the Security Services Act 1989[59] or the Intelligence Services Act 1994[60].

11.11 Our review and this report highlight clearly the difficulties when statutes are operated in secret and where there is a lack of statutory codified procedures. We have made extensive recommendations throughout this report which must be implemented to clarify and bring consistency to the procedures in place, remedy the lack of record-keeping requirements and ensure that we are able to undertake our oversight of the giving and use of section 94 directions properly. The recommendations are listed in the next section of the report. The Commissioner requires the public authorities and, where relevant, the PECNs to implement the recommendations without delay.

[59] See sections 1 and 2 http://www.legislation.gov.uk/ukpga/1989/5/contents
[60] See section 3 and 4 http://www.legislation.gov.uk/ukpga/1994/13/contents

Section 12

Recommendations

Recommendation 1

Each public authority must keep a central record of all section 94 directions given by any Secretary of State on their behalf. The central record must include the date the direction was given; the name of the Secretary of State giving the direction; the PECN to which the direction relates and the date the direction was served on the PECN; a description of the conduct required to be undertaken; and the date the direction was cancelled. The central record must be available for inspection by IOCCO.

Recommendation 2

Each time a section 94 direction is given by a Secretary of State it must be notified to the Commissioner by the public authority. In order to enable a reverse audit to be conducted, each time a section 94 direction is served on a PECN, the PECN should report the details of that direction to the Commissioner.

Recommendation 3

All section 94 directions for bulk communications data should indicate the specific communications data that is required to be disclosed by the PECN. When a requirement is amended (i.e. modified) a new direction should be given.

Recommendation 4

There should be a clear mandated application process for section 94 directions which sets out the requirements to be met. The public authorities (in consultation with the Home Office and Foreign & Commonwealth Office) should develop a specimen application form template and a specimen section 94 direction template in order to ensure a standard and consistent approach.